DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

DEFENSE SWITCHED NETWORK INFORMATION ASSURANCE TEST PLAN
Version 2

JANUARY 2009

DEFENSE SWITCHED NETWORK
INFORMATION ASSURANCE
TEST PLAN

MAY 2009

Submitted by: Joseph Schulte
Chief, Network Systems Branch

Approved by: ______________________________
RICHARD A. MEADOR
Chief, Battlespace Communications Portfolio

Prepared Under the Direction of:

Michael Napier
Joint Interoperability Test Command
Fort Huachuca, Arizona

(This page intentionally left blank.)

EXECUTIVE SUMMARY

The Department of Defense (DoD) Directive 8500.1 “Information Assurance (IA),” 24 October 2002, established the DoD policies for IA and directed that all information technology be IA tested and certified before connection to the Defense Information System Network (DISN). The DoD Instruction 8100.3, “Department of Defense Voice Networks,” 16 January 2004, establishes the IA policy for DoD Voice Networks, including the Defense Switched Network (DSN). The DSN Single Systems Manager (SSM) is responsible for providing DSN IA test results to the DISN Designated Approving Authorities in order to be granted IA certification and accreditation. The DSN SSM has designated the Joint Interoperability Test Command (JITC) as the responsible organization for DSN IA testing.

The JITC DSN IA Test Team (IATT) supports IA testing by determining compliance with the Security Technical Implementation Guidelines, IA Vulnerability Management announcements (e.g., alerts, bulletins, and technical guidance), and additional IA requirements. In addition, the IATT scans for Internet Protocol Vulnerabilities to determine residual risks and threat levels of the existing security implementations and any security deficiencies on the network.

Upon completion of the IA assessment, the IATT analyzes data collected and presents the test findings in an “IA Assessment Findings and Mitigations Report.” The report contains security vulnerabilities found on the system during the test. The report is emailed to the vendor so they may input their mitigation strategies for the security vulnerabilities found. The assessment report, including the vendor’s mitigation strategies is submitted to the Unified Capabilities Connection Office and the Defense Information Systems Agency (DISA) Field Security Office (FSO) for comment. The FSO will write a Certification and Accreditation letter to the DISN Security Accreditation Working Group (DSAWG). The final assessment report is briefed to the DSAWG in the form of a PowerPoint presentation. The DSAWG will decide whether to place the vendor’s solution on the DSN Approved Products List, based on the findings and mitigations.

(This page intentionally left blank.)

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (continued)

APPENDICES

LIST OF FIGURES

TABLE OF CONTENTS (continued)

LIST OF FIGURES (continued)

Page

LIST OF TABLES

TABLE OF CONTENTS (continued)

LIST OF TABLES (continued)

Page

SUMMARY OF CHANGES

Editor/Approver	Date	Purpose
Brent Searle/ Donna Quick-Keckler	13 March 2008	Removal of the GR-815 CORE test procedures and the incorporation of the GR procedures into the associated STIG.
Kirsten Kimbler/ Donna Quick-Keckler	15 January 2009	Addition of the Protocol Analysis test tool, Spectra, and training procedures.

INFORMATION ASSURANCE DESCRIPTION

The Department of Defense (DoD) Directive 8500.1 “Information Assurance (IA),” 24 October 2002, established the DoD policies for IA and directed that all information technologies be IA tested and certified before connection to the Defense Information System Network (DISN). The DoD Instruction (DoDI) 8100.3, “Department of Defense Voice Networks,” 16 January 2004, establishes the IA policy for DoD Voice Networks, including the Defense Switched Network (DSN). The DSN Single Systems Manager (SSM) is responsible for providing DSN IA test results to the DISN Designated Approving Authorities to grant IA certification and accreditation. The DSN SSM has designated the JITC as the responsible organization for DSN IA testing.

There are four possible IA phases for IA testing. The first is the Security Technical Implementation Guidelines (STIG) testing phase, which assesses the system’s ability to operate reliably in a secure environment. Within this phase additional IA requirements are also tested. Additional IA requirements are those requirements that were cross-referenced with the General Requirements (GR)-815 CORE requirements that are no longer in use. A listing of these requirements can be found in Appendix E. The Internet Protocol (IP) Vulnerability (IPV) phase covers the system’s ability to resist attack and determines whether the system operates securely in an IP network. The third phase of testing is Protocol Analysis (PA), which evaluates the system for its ability to maintain confidentiality, integrity, and availability of legacy Time Division Multiplexing (TDM) protocols that include SS7, Basic Rate Interface (BRI), and Primary Rate Interface (PRI), when communicating with distant end switches or local end instruments. If applicable an additional phase, Internet Protocol version 6 (IPv6) requirements are assessed against the system. IPv6 verifies that the tested system can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/v6 environments. Appendix B lists the requirements used for assessments and Appendix E lists specific procedures for each phase of testing. Appendix B will also include those appliances that will have IPv6 requirements assessed against them.

The architecture of the DSN is a two-level network hierarchy consisting of backbone switches and infrastructure (managed by the Defense Information Systems Agency) and installation switches and peripherals (managed by military departments and agencies). Appendix D, Figure D-1, illustrates the detailed DSN architecture.

This two-level network hierarchy includes the following: The first level consists of components that are backbone switches and network transportation devices which includes Tandem Switches, Multifunction Switches (MFS), Signal Transfer Points (STP), Network Management Systems, End Office Switches, and Small End Office Switches. The second level is the installation switches and customer premise edge equipment to include local peripherals, which consists of Deployable Voice Exchanges, Remote Switching Units, Private Branch Exchange (PBX) Types 1 and 2, Video Teleconferencing, Customer Premise Equipment (CPE), Edge Border Controllers, Network Elements, Echo Cancellers, Integrated Access Switches/Systems, Assured Services Local Area Networks, and Conference Bridges.

The DSN provides end-to-end command and control capability via dedicated telephone service, facsimile, voice-band data, dial-up firewalls, and Transport Layer Security. The DSN comprises backbone and tandem switches, signaling system instruments, transmission connectivity between switches, installation switches, network management systems, and end devices. Voice processing and transport technologies such as Voice over Internet Protocol (VoIP) and Voice over Asynchronous Transfer Mode are also elements of the DSN.

INFORMATION ASSURANCE BACKGROUND

Vendors are continuously developing new features and functions to meet user demands and to correct any deficiencies within the solution. As of January 2004, DoDI 8100.3 mandates all systems that connect to or will connect to the DSN, undergo IA certification. The Unified Capabilities (UC) Approved Products List (APL) is a list of equipment authorized by the DoD to be fielded in the DISN. The first part of the APL Certification Process is IA accreditation testing. If the solution meets the requirements for IA accreditation, it continues to the second part of the test cycle, Interoperability (IO) testing. When IA accreditation and IO certification is granted, the solution is then included on the UC APL.

To enhance the vendor's IA posture and readiness strategy, JITC conducts IA assessments of vendors' products before they undergo IO certification. Program Managers or DoD agencies must obtain IA accreditation for all telecommunication equipment that is being procured for use on the DSN, whether the equipment is new or is an updated version of equipment already in the DSN. All DoD information systems must identify, implement, and manage IA controls based on the DoD Information Assurance IA Certification & Accreditation (C&A) Process (DIACAP), reference Appendix B, paragraph B-5.

DEFENSE-IN-DEPTH AND REQUIRED ANCILLARY EQUIPMENT (RAE)

The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigations is through: the integration of people, technology, and operations; the layering of IA solutions within and among Information Technology (IT) assets; and the selection of IA solutions based on their relative level of robustness. This combination produces layers of technical and non-technical solutions that do the following: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response.

The use of RAE components can aid the site in developing and implementing its Plan of Action and Milestones to supplement the DIACAP accreditation package. Use of this equipment or software provides additional security features to the existing environment, which may already be present in a government infrastructure and enforce defense-in-depth. As a minimum, RAE may consist of one or a combination of the following:

1. Microsoft Windows Server 2003 Internet Authentication Service Remote Authentication Dial-In User Server (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+)
2. Active Directory
3. SysLog Server
4. Public Key Infrastructure

INFORMATION ASSURANCE PURPOSE

The purpose of this IA assessment plan is to provide a consistent set of guidelines for testers and developers to evaluate the operation of any switch system to the applicable STIG, additional IA requirements, IPV6, and IPV/Protocol Analysis (PA) requirements.

REQUIREMENTS

Government regulations include all aspects of IA, including the acquisition, deployment, and use of IA or IA-enabled IT products. Appendix G contains the full list of references for these requirements.

SCOPE

The IA test plan covers traditional telecommunications (Time Division Multiplexing) components along with IP-enabled or IP-centric solutions. Most vendors are moving toward unified capabilities that function in an IP environment, while continuing to support legacy capabilities. As systems continue to migrate from a traditionally large hardware driven platforms to smaller software driven platforms, vulnerability analysis of the customized software and applications requires a specialized approach. The JITC IA process for evaluating these unified capabilities products aides in determining the security posture of individual IP-enabled products connected to the network. The IA phases of testing consist of the following:

- **Phase I: STIG and Additional IA Requirements.** Phase I testing involves applying predetermined STIG and additional IA requirements to various components of the vendor solution, and recording any vulnerabilities found during the test. The STIG applicability is determined by attributes such as the underlying operating system of the solution (e.g., Windows, Linux, or UNIX), applications or services that operate on the solution, and the type of solution (e.g., MFS, PBX, router, switch, or server). A solution may require the application of one or more STIGs. The lab assessment contains a DIACAP control correlation matrix (scorecard) that addresses DoD IA controls. The DIACAP package along with the IA report can assist the site in creating and implementing a security baseline, providing a foundation for achieving its Interim Authority to Operate. Both requirements and implementation procedures are discussed in Appendices B and F, respectively.

- **Phase II: IP Vulnerability Scans/Protocol Analysis.** Phase II consists of scanning and/or attacking the vendor's solution using the tools available to an attacker intent on penetrating a network or system. Vulnerability analysis for custom software or applications protocols such as Signaling System 7, Primary Rate Interface, Channel Associated Signaling, European Carrier 1 (E1), Telecommunications Carrier 1 (T1) Session Initiation Protocol, and Secure Real-time Transport Protocol (SRTP) may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, and statistical analysis of source code). The scan results are packaged in human-readable form in Portable Document Format (PDF) and are part of the DIACAP submission. Appendices B and F contain detailed procedures.

- **Phase III**: **Protocol Analysis.**

- **Phase IV**: **Internet Protocol version 6. (if applicable)**

LIMITATIONS

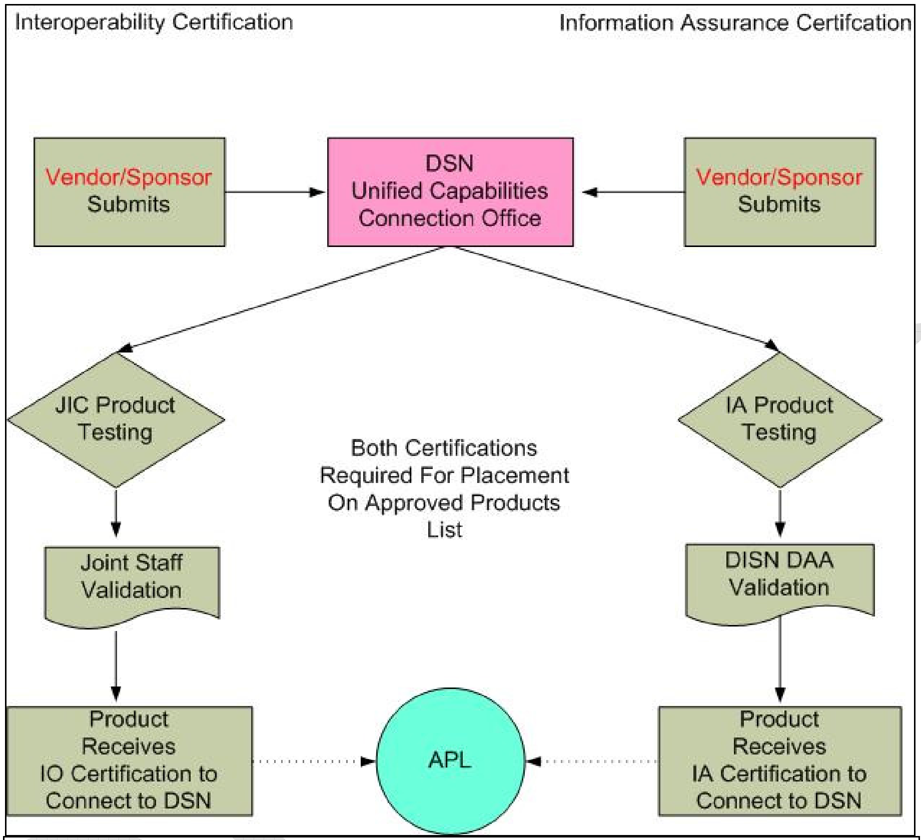
Portions of the STIG's may not be assessed due to limitations in the System Under Test (SUT) not being deployed in an operational environment. The DIACAP Scorecard shows these items as "site responsibility" or "not applicable" for the SUT. Some of these items include aspects of enclave security, personnel qualifications, training, and contingency planning (e.g., disaster recovery plans, backups, storage of media, and incident reporting). The APL assessments include local network and firewall configuration and meet appropriate standards. As part of the local certification and accreditation package the installers should assess these items, as well as other DoDI 8500.2 IA Controls in addition to local site requirements.

METHODOLOGY

The APL IATT performs certification assessments utilizing the methodologies presented in this plan. The methods cover Phase I and Phase II IA testing, including STIG testing and additional IA requirements, IPV scanning tests, PA SS7, SIP, H.323, and SRTP protocol analysis testing.

Certification Process Overview. Figure 1 depicts the IA and IO APL product certification process flow. When a sponsor desires to have a vendor's product evaluated, the vendor contacts the Unified Capabilities Certification Office (UCCO). The UCCO has standard procedures for processing vendor requests for placement on the APL testing cycle. These detailed procedures are documented by the UCCO at <http://www.disa.mil/gs/dsn/jic/index.html> as part of the APL Test Bundle.

Part One of the APL Certification Process is the IA certification testing. If the product does not meet the requirements for IA certification, the solution is returned to the vendor for correction and the testing cycle starts over. If the solution meets the requirements for IA certification, it then continues with Part Two of the test cycle, IO testing.


Interoperability Certification
Information Assurance Certifcation
Vendor/Sponsor Submits
DSN Unified Capabilities Connection Office
Vendor/Sponsor Submits
JIC Product Testing
IA Product Testing
Both Certifications Required For Placement On Approved Products List
Joint Staff Validation
DISN DAA Validation
Product Receives IO Certification to Connect to DSN
APL
Product Receives IA Certification to Connect to DSN

LEGEND:

APL	Approved Products List	IA	Information Assurance
DAA	Designated Approving Authority	IO	Interoperability
DISN	Defense Information System Network	JIC	Joint Intelligence Center
DSN	Defense Switched Network		

Figure 1. APL Certification Process Flow

The following is a brief overview of the UC IA testing process and provides the vendor a starting point:

- Coordinate payment of lab testing fees/ Cooperative Research And Development Agreement (CRADA) agreements with Action Officer (AO).

- Download APL Test Bundle at <http://www.disa.mil/dsn/jic/>. Review bundle and submit documentation In Accordance With the APL Documentation Guide, which is included in the APL Test Bundle.

- Apply applicable STIGs and submit to UCCO within 2 weeks before scheduled test window.

- The UCCO receives and reviews the test submittal package from the applicant. A tracking number is assigned to the solution and the package is provided to the Government AO. The Action Officer will contact the vendor with further instructions.

- Provide on-site engineering support for the SUT during all phases of testing.

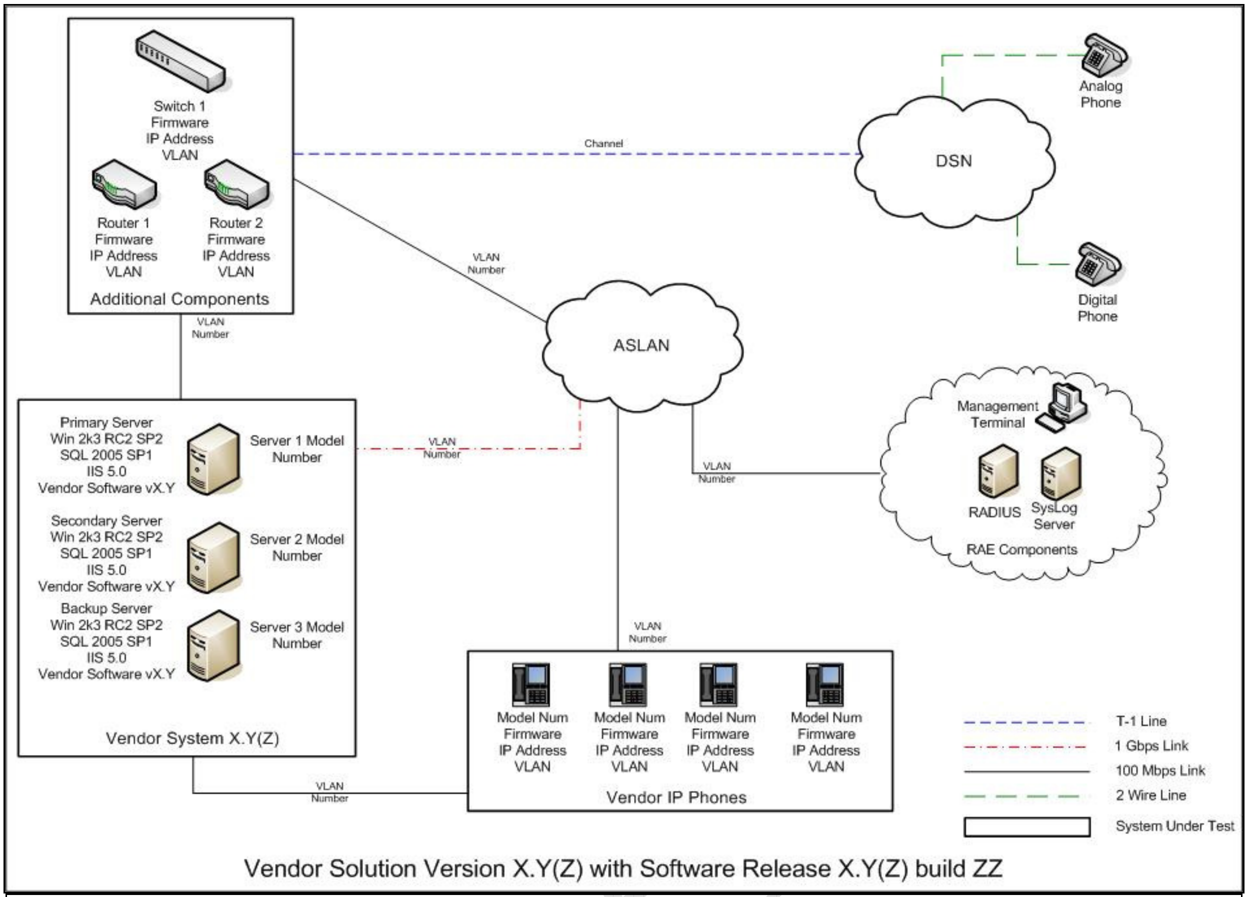
- Once the DSN-UCCO has assigned the vendor a tracking number, the DSN-UCCO in coordination with the IATT will assign testing dates. The vendor is required to submit a self-assessment report.

TESTING METHODOLOGY

This section describes the methodology used and the steps taken during the various phases of testing. Due to the sensitive nature of testing, all data collected is treated as sensitive and exempt from the Freedom of Information Act. All tests consist of obtaining vendor documentation, conducting an official initial contact meeting, which provides the test requirements, conducting a functionality test before and after each phase of testing, and then conducting an outbrief, which leads to the Final IA Assessment Report. Appendix E contains detailed procedures.

Documentation. Reviewing vendor documentation is vital to successful testing. While testing every possible scenario within the vendor scope is not possible, understanding the product's general use, features, and functionality assists the test team in its evaluation. The documentation and information includes the vendor's web page, product manuals, whitepapers, newsgroups, forums, user mailing lists, and vendor self-assessments. The team reviews these, as well as other documents, to understand the products they are evaluating and to find possible weaknesses and vulnerabilities that may have been discovered by other sources.

The Test Preparation document generated during the first phase of testing contains the vendor and tester contact information, IP addresses, test equipment hardware, software and version information, IP phone information, and other applicable information to the testers. Figure 2 depicts a sample vendor diagram that is used to aid the tester and reader in understanding how the system interconnects. An example of the test preparation document is located in Appendix C, Test Preparation Document. The signature page of this document clarifies that all hardware, software, and version information is correct. The testers sign and deliver the packet to the next phase of testing tester when they are finished; when all IA phases are completed, the packet is turned over to the IO tester for verification and is used to minimize duplicate efforts. The vendor and the testers will verify all hardware and software before IO Testing begins.



LEGEND:

ASLAN	Assured Services Local Area Network	RAE	Require Ancillary Equipment
DSN	Defense Switched Network	SP	Service Pack
Gbps	Giga-bytes per second	SQL	Structured Query Language
IIS	Internet Information Service	T-1	T-Carrier 1
IP	Internet Protocol	VLAN	Virtual Local Area Network
Mbps	Mega-bytes per second	Win	Windows
MS	Microsoft	Win2k	Windows 2000
Num	Number	Win2k3	Windows 2003
RADIUS	Remote Authentication Dial-in User Server/Service		

Figure 2. Sample Diagram

Functionality Tests. Testing the SUT's functionality ensures that the product operates as designed in a fielded production environment. Results due to services not functioning correctly, disabled services, and applications not communicating correctly can provide a false sense of security because not all aspects of the test product were evaluated. Completing the functionality test at the beginning and end of every phase of testing ensures that any settings or changes made during testing did not affect the functionality of the product. Functionality testing will vary from test to test, depending on the SUT. The functionality test will target basic operational functions. It is not an interoperability test.

Some products, such as CPE, rely on external systems to exercise their capabilities. For example, a secure modem solution does not function unless an external switch initiates a call. In this case, the external switch is outside the scope of the IA test; however, the tester and vendor must ensure it is operational to perform testing on the secure modem solution. While conducting functionality tests, IP traffic is monitored (sniffed) and saved at the conclusion of the functionality test for further evaluation, if necessary.

Security Technical Implementation Guidelines (STIG) Assessment Methodology. The DoD uses STIG's to strengthen and assess the security posture of a system or component. Findings resulting from applying the Gold Disks and scripts are indications of weaknesses in the security posture of the system or component. Findings from the STIG's are grouped into three Categories (CAT) based on the severity of the weakness. The findings will correspond to IA Controls that are listed in Appendix B and annotated on the DIACAP Scorecard, as shown in Appendix E. The scorecard is a summary report illustrating the certified or accredited implementation status of a DoD information system's assigned IA Controls. It supports or conveys a certification determination and/or accreditation decision. The DIACAP Scorecard is intended to convey information about the IA posture of a DoD information system in a format that can be easily understood by managers and be easily exchanged electronically. The DIACAP is the DoD process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, federal, and DoD requirements. The following list shows the high-level procedures for Phase I testing:

1. **Apply STIG/Security Readiness Reviews (SRR)/Checklists**

   - Validate SUT is operational and conduct functionality checks before starting the assessment.
   - Determine the Management Interface—The management interface contains software that maintains the SUT and its underlying capabilities. This may consist of multiple software applications. Consider any additional software application(s) that manage hardware associated with the solution that are a management interface or control panel.
   - The DoDI 8500.2 defines Mission Assurance Category (MAC) I as "Systems categorized as 'MAC I' process data that is vital to the operational readiness or mission effectiveness in terms of both content and timeliness. MAC I systems require high confidentiality, integrity, and availability to accomplish their missions; therefore, they are categorized as critical network components." The IATT always tests the SUT at the MAC I level. The confidentiality level is always Sensitive But Unclassified for the SUT.

2. Collect Data

- Document findings
  - Note any findings deemed not applicable
  - Note any fixes performed by the vendor
  - Note any findings deemed as false positives
- Document test limitations
- Validate SUT is operational and conduct functionality checks after completion of assessment

3. Perform Data Analysis and Report Results

Data collected from the STIG, their respective Checklists, and any SRR scripts will be analyzed to accomplish the following assessment objectives:

- Identify and attempt to eliminate "false positive" results.
- Highlight and categorize findings according to their level of importance, whether vulnerabilities are CAT I (high), CAT II (medium), or CAT III (low).
- Provide recommendations to remediate or mitigate the risks.

Additional IA Testing Methodology. The design of IA Generic Requirement (GR)-815 CORE testing focuses on the proper protection of the SUT's control panel, security log, and transferred data through encryption, as well as conformance to acceptable security standards. The test team incorporated GR-815 requirements to STIG requirements, and developed additional test procedures in the DIACAP Scorecard to address GR-815 requirements that are not validated via the STIGs. There are 19 test procedures included in Appendix E, to support GR-815 requirements testing not supported by STIG.

Unified Capabilities Requirements (UCR) IA Internet Protocol version 6 (IPv6) Methodology. The UCR IA IPv6 Requirements section is used to verify that the tested system can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/v6 environments. The UCR IA IPv6 requirements have been implemented relating to voice telecommunications equipment specific to IPv6 Profile Categories. Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only IPv4, only IPv6, or both IPv4 and IPv6. An IPv6 capable network shall be ready to have IPv6 enabled for operational use, when mission need or business case dictates. Specifically, an IPv6 capable network must meet the following:

a. Use IPv6 Capable Products.

b. Accommodate IPv6 in network infrastructures, services, and management tools and applications.

c. Conform to DoD and NSA-developed IPv6 network security implementation guidance.

d. Manage, administer, and resolve IPv6 addresses in compliance with the DoD IPv6 Address Plan when enabled.

e. System Requirements, Maximum Transmission Unit (MTU), Flow Label, Address, Dynamic Host Configuration Portal (DHCP), Neighbor Discovery, Redirect Messages, Router Advertisements, Stateless Address Autoconfiguration and Manual Address Assignment, Internet Control Message Protocol (ICMP), Routing Functions, IP Security, Network Management, IP Version Negotiation, AS-SIP IPv6 Unique Requirements, and Miscellaneous Requirements.

IP Vulnerability (IPV) Testing Methodology. The IPV test team conducts vulnerability assessments and penetration testing for Approved Products List (APL) telecommunication equipment destined for connection to the DSN.

The design of a vulnerability assessment is to analyze the system in scope and find areas where attacks might be more likely to occur, without necessarily exploiting the problems identified. A vulnerability assessment typically involves investigation of the Operating System to determine whether current patches are applied, whether the system is configured in a manner that makes attacks more difficult, and whether the system exposes any information that an attacker could use to exploit other systems in the enclave. Vulnerability assessments use a number of commercial and proprietary tools to minimize false positives.

The design of a penetration test is to simulate an attack on the vendor's system within a specified environment. While a number of variables determine how the attacks are initiated and conducted, the defining characteristic of a penetration test is that IA testers will be actively attacking the system using the same or similar methods to what an actual attacker would use.

The following DoDI 8500.2 IA Controls apply to the IPV testing procedures: Design and Configuration Ports Protocols and Services (DCPP-1), Enclave and Computing Environment Voice over IP (ECVI-1), Enclave and Computing Environment Transmission Integrity Controls (ECTM-2), Vulnerability and Incident Management Vulnerability Management (VIVM-1), and Enclave and Computing Monitoring and Testing (ECMT-1).

The IPV test team conducts vulnerability scanning with penetration tools and techniques. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for application, source code reviews, and statistical analysis of source code). The following steps outline the general procedures that the test teams employ. Appendix E contains detailed procedures.

1. Perform Identification and Verification

- IP Interface Identification – Identify and verify all operational IP interfaces.

2. Determine Test Components

- If the system supports lines, the following manual calls should be attempted: Analog to Analog, IP to IP, Analog to IP, and IP to Analog. Confirm that all test calls are completed and all IP handsets are identified.

- Trunks allow a group of inlet switches or circuits to connect at the same time. The service provider can provide a lesser number of circuits than might otherwise be required, allowing many users to “share” a smaller number of connections and achieve capacity savings. If the system supports trunks, the following manual calls should be attempted: Analog over trunk and IP over trunk. Confirm that all test calls were completed.

3. Discover Host

Finding all the hosts in use by the system is the first step in the technical evaluation. Detecting all the possible hosts and their corresponding IP address information is required to begin any further technical evaluation.

4. Conduct Ping Sweep

A general ping sweep will determine what hosts are available via the Internet Control Message Protocol (ICMP). This is generally an ICMP echo request (type 8) to elicit an ICMP echo reply (type 0) from a host.

5. Conduct Transmission Control Protocol (TCP) Sweep

The TCP sweep provides insight into available hosts when ICMP is disabled. A TCP sweep will attempt to make TCP connections to a host range on a specified port list. The client will send a Synchronize (SYN) and, if the host is available on that port, the client will receive a SYN/Acknowledge (ACK) and respond with an ACK packet to the target host with a sequence number incremented by one.

6. Perform Traffic Analysis

Traffic Analysis allows the test team to determine all the hosts that are included within the solution under test.

7. Perform Port Enumeration

Port enumeration provides a list of services or applications that could be running on the host and gives the tester a good indication of what operating system might be present on the end-point. Port scanning of each host will provide a detailed list of which ports are open, closed, or filtered on a specified host. Conduct port scans using many different protocols, packet flags, and techniques. These different scans can yield different results in different situations, depending on the configurations and protections of each host. Additional Open Source Security Testing Methodology Manual strategies are in Appendix E.

8. Conduct Service Enumeration

Service Enumeration determines what services are listening on an IP port of the system. Services and their versions can provide the tester with a list of known exploits or weakness that might be effective against a given target.

9. Perform Service Analysis

The use of Service Analysis provides the test team with specific service details used in further attacks. Upon discovery of a service, a variety of checks may be completed against a known service.

10. Evaluate Denial of Service (DoS)

A DoS evaluation determines the system's susceptibility to attacks. The testing team might take a particular end-point offline to capture one of its attributes, such as an IP address or Media Access Control address.

11. Package for DIACAP

Package all raw results generated from the test into a human-readable format and add to the report.

Protocol Analysis (PA). The test team conducts generic PA requirements for the APL inclusion. Additional specifications include those found in American National Standard Institute T1.111 through T1.116. The system is evaluated for its ability to maintain confidentiality, integrity, and availability. Detailed test procedures are in Appendix E.

OUTBRIEF. After the conclusion of all phases of testing and the vendor has provided mitigations to all open findings, the draft report is discussed with the vendor, IATT, sponsor, UCCO, and Field Security Officer (FSO). All findings are reviewed, questions about specific findings are discussed, and any outstanding issues are assigned as action items to the respective party. During the outbrief the vendor, IATT, sponsor, UCCO, and FSO review the supplied network configuration, the hardware, and software to ensure that it is correct before accreditation is considered.

Following the outbrief meeting and the completion of all action items, a final report is prepared and submitted for approval by the government Action Officer. Copies are distributed to all parties, including the FSO for the Certifying Authority's recommendation letter of the SUT to the DISN Security Accreditation Working Group for placement on the APL. Scan and test results are provided as baseline examples for sites to use when assessing their solutions and creating their DIACAP artifacts.

EXAMPLE RESULTS

Results that testers document in the draft IA Findings and Mitigations Assessment Report are shown in the example below. Findings from each STIG, IA Requirements, and Penetration testing requirement with and without RAE influence the vendor's system. All findings will show each component affected by the finding and any findings that the vendor or sponsor mitigated by secure RAE. The findings with RAE are the remaining number of findings inherent to the system. Each finding will show the security requirement, associated vulnerability, and impact of the vulnerability. Section 5, Summary, shown below, is from an actual result findings report of a SUT; however, actual test results have been removed and annotated with fields marked "##".

> **5. SUMMARY.** Table 1 depicts critical testing requirements and summary findings that were identified while undergoing Defense Switched Network (DSN) Approved Products List (APL) certification. A finding is a discrepancy requiring investigation for a potential vulnerability that could be exploited given certain conditions. An analysis of each finding must be conducted to determine its impact to the overall security posture of the system under test. The findings listed in the column without secure Required Ancillary Equipment (RAE) (W/O-RAE), see Appendix, are the total number of findings present within the system. These findings would be present if a defense in depth strategy or any other mitigations are not applied by the site acquiring this product. The findings in the column with RAE (W-RAE) are the remaining number of findings inherent to the system. If properly fielded with secure RAE, which comprise equipment installed and maintained in a secure facility in accordance with enclosure 4 to Department of Defense Instruction (DoDI) 8500.2, "IA Implementation," dated 6 February 2003, can be eliminated. Additional details are found in paragraph 13, Test Results and IA Findings, explaining which secure device and vendor mitigations needs to be used to mitigate the specific finding.

Table 1. SUT IA Test Summary

Requirement	Critical	W/O-RAE	W-RAE	Page Number
STIG	Yes	## Findings ## CAT I ## CAT II ## CAT III	## Findings ## CAT I ## CAT II ## CAT III	8
IPV	Yes	## Findings ## High Risk ## Medium Risk ## Low Risk	## Findings ## High Risk ## Medium Risk ## Low Risk	45

LEGEND:

CAT	Category	STIG	Security Technical Implementation Guidelines
IA	Information Assurance	SUT	System Under Test
IPV	Internet Protocol Vulnerability	W	With
RAE	Required Ancillary Equipment	W/O	Without

(The page intentionally left blank.)

APPENDIX A

ACRONYMS

ACL	Access Control Lists
ACK	Acknowledge
ANSI	American National Standards Institute
AO	Action Officer
APL	Approved Products List
C&A	Certification & Accreditation
CA	Certifying Authority
CAT	Category
CIS	Center for Internet Security
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CPE	Customer Premise Equipment
CRADA	Cooperative Research And Development Agreement
DAA	Designated Approving Authority
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoS	Denial of Service
DSAWG	DISN Security Accreditation Working Group
DSN	Defense Switched Network
E-1	European Digital Signal Level-1
FIN	Finish
FIPS Pubs	Federal Information Processing Standards Publications
FISMA	Federal Information System Management Act
FOS	Fixed On Site
FSO	Field Security Officer
GIG	Global Information Grid
GNTF	Global Information Grid Network Test Facility
GR	Generic Requirement
HTML	HyperText Markup Language
IA	Information Assurance

IAM	Information Assurance Manager
IASE	Information Assurance Support Environment
IATT	IA Test Team
ICMP	Internet Control Message Protocol
ID	Identification
IO	Interoperability
IP	Internet Protocol
IPV	IP Vulnerability
IS	Information System
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IT	Information Technology
JITC	Joint Interoperability Test Command
LS	Link Set
MAC	Mission Assurance Category
MFS	MultiFunction Switch
MMC	Microsoft Management Console
NA	Not Applicable
NF	Not a Finding
NIAP	National Information Assurance Partnership
NIPRNet	Unclassified-But-Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NR	Not Reviewable
NSA	National Security Agency
OS	Operating System
OSSTM	Open Source Security Testing Methodology Manual
PA	Protocol Analysis
PBX	Private Branch Exchange
PDF	Portable Document Format
Ping	Packet Internet Groper
POA&M	Plan of Action and Milestones
RADIUS	Remote Authentication Dial-In User Server
RAE	Required Ancillary Equipment
RAM	Random Access Memory
RST	Reset
SA	System Administrator
SAPI	Service Access Point Identifier
SIP	System Identification Profile

SLC	Signaling Network Management
SP	Signaling Point
SQL	Structured Query Language
SRR	Security Readiness Review
SRRDB	Security Readiness Review Database
SRTP	Secure Real-Time Protocol
SS7	Signaling System Number 7
SSM	Single Systems Manager
STIG	Security Technical Implementation Guidelines
STP	Signaling Transfer Point
SUT	System Under Test
SYN	Synchronous
T-1	Telecommunications Carrier 1
TACACS+	Terminal Access Controller Access Control System Plus
TBD	To Be Determined
TCP	Transmission Control Protocol
UC	Unified Capabilities
UCCO	Unified Capabilities Connection Office
V&V	Verification and Validation
VSP	Virtual Signaling Point
XP	Experience

(The page intentionally left blank.)

APPENDIX B

REQUIREMENTS

The requirements for assessing the Information Assurance (IA) security posture Information System (IS) are from the following documents: Security Technical Implementation Guides (STIG), Gold Disks, Security Readiness Review (SRR) scripts by the Defense Information Systems Agency (DISA) and National Security Agency (NSA), Operating System Security Guides, NSA Router, Switch Guides, and Microsoft Security Guides for Microsoft-based software. The baseline for security Department of Defense (DoD) IA is established by the requirements in DoD Directive (DoDD) 8500.1 and DoD Instruction (DoDI) 8500.2. In addition, the IA Security Standards testing is designed to focus on the proper protection of the System Under Test's (SUT) control panel, security log, and transferred data through encryption, as well as conformance to acceptable security standards. Section B-2 lists all requirements applied within this phase. Finally, many different methods and tools can successfully perform Internet Protocol Vulnerability (IPV) testing.

B-1. SECURITY TECHNICAL IMPLEMENTATION GUIDELINES (STIG). The DoD uses STIG to strengthen and assess the security posture of a system or component. Findings resulting from running the Gold Disks and scripts are indications of weaknesses (or "holes") in the security posture of the system or component. Findings from the STIG are grouped into three Categories (CAT) based on the severity of the weakness. **CAT I** findings are those that allow an attacker to gain immediate access to a system or component, allow elevating a user's rights to administrator (or super user) level, or allow bypassing a firewall. These are the most severe findings. Systems or components having multiple CAT I findings may not be accepted for additional testing or for placement on the Unified Capability (UC) Approved Products List (APL). **CAT II** findings are those that provide information about the system or component and therefore have a high potential of allowing unauthorized access to an intruder (the more that is known about a computer or system, the easier it is to find the weaknesses in the hardware, firmware, or software). **CAT III** findings are those that give away enough information for an intruder to compromise the system or component. High numbers of CAT II and III findings may indicate an overall weakness in the security posture of the system or component and may preclude placement on the UC APL. Table B-1 provides the description for each STIG. Figure B-1 is a screenshot from DISA's Information Assurance Support Environment (IASE) website

Table B-1. STIG Listing

STIG	Description
Access Control STIG	Access Control STIG details a security framework for use when planning and selecting access control for protecting sensitive and classified information in the DoD. It provides a consolidated starting place for the security planning team responsible for ensuring compliance with DoD policies. This STIG presents a practical methodology for selecting and integrating logical and physical authentication techniques while tying the solution to the asset's value, environment, threat conditions, and operational constraints. For classified access, the solution must protect access to sensitive or classified systems and data while considering the need for appropriate and authorized access in uncontrolled areas for DoD personnel, contractors, and coalition forces.
Application Security and Development Checklist	Application Security and Development Checklist is used for custom developed software, either COTS or Government Off The Shelf, and the programming code used for the application that resides on top of an OS. The checklist covers all aspects of the application, including identification, authentication, interaction with ActiveX, Java, e-mail clients, web browsers, session logging, auditing, and enclave impact.
Application Services STIG/Checklist	Application Services STIG provides security configuration and implementation guidance for application server products designed to comply with the J2EE™. The J2EE defines a standard security framework of configuration and implementation for the protection of application servers.
Backbone Transport Services STIG	Backbone Transport Services STIG provides IA guidance and addresses security issues relating to the Global Information Grid backbone network. Guidance in this STIG is provided for all transport components, their relationships, interoperability, and principles used for governing their configuration, implementation, management, and operation.
Biometrics STIG	Biometrics is used to enhance security; however, there are security risks associated with it, which must be mitigated. The Biometrics STIG provides guidelines for implementing technological systems, such as biometrics.
Database STIG	Database STIG provides the technical security policies, requirements, and implementation details for applying security concepts to database servers. It generally covers all database servers and specifically Oracle, Microsoft SQL Server, and DB 2 servers supporting data storage and retrieval from local, intranet, or Internet clients.
Defense Switched Network (DSN) STIG	DSN STIG provides the technical security policies, implementation details, and requirements for applying security concepts to the DoD telecommunications systems. The DSN encompasses inter-base and intra-base non-secure and/or secure C2 telecommunications systems that provide end-to-end common use and dedicated telephone service, voice-band data, and dial-up Video Teleconferencing for authorized DoD C2 and non-C2 users. Non-secure dial-up voice (telephone) service is the system's principal requirement. The span or scope of the DSN covers the CONUS and a large portion of the world outside of the CONUS.
Desktop Application STIG	Desktop Application STIG provides the technical security policies, requirements, and implementation details for applying security concepts to COTS applications on desktop workstations. This STIG also applies to the lock-down procedures for Exchange Servers.
Defense Red Switch Network (DRSN) STIG	DRSN STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the DRSN. This STIG is directive in nature and applies to all DoD components and government agencies, including their contractors that are served by the DRSN, or whose RED (secure) switch interconnects with the DRSN.
Directory Services STIG	AD Security Checklist provides the procedures for conducting a SRR to determine compliance with the requirements in the AD STIG. This Checklist document must be used together with the corresponding version of the STIG document. As in the related STIG, this Checklist addresses three review subjects: 1. AD Implementation - This subject covers checks for AD Domain Controllers, AD Domains, and the AD Forest that make up an implementation of Active Directory. 2. Synchronization/Maintenance Application - This subject covers checks for an individual installation of an application used to perform synchronization or maintenance on one or more AD implementations. 3. ADAM - This subject covers checks for an individual installation of ADAM as a directory service.
Domain Name System (DNS) STIG	Domain Name System STIG is designed to assist administrators with configuration DNS server software and related portions of the underlying operating system. This STIG also provides guidance for standard operating procedures related to configuration management, business continuity, and other topics.
Enclave STIG	Enclave STIG security provides the information protection guidance necessary to implement secure IS and networks while ensuring interoperability. This STIG includes security considerations at the network level needed to provide an acceptable level of risk for information transmitted throughout an enclave.
Enterprise Resource Planning (ERP) STIG	ERP STIG provides the technical security policies, requirements, and implementation details for COTS ERP application software. For this STIG, ERP software will refer to all commercially available software packages that supply one or more of the functions generally found within ERP packages. The functions include but are not limited to Human Resources, Financial processes, Customer Relations Management, sales, warehousing, inventory control, and manufacturing.

Table B-1. STIG Listing (continued)

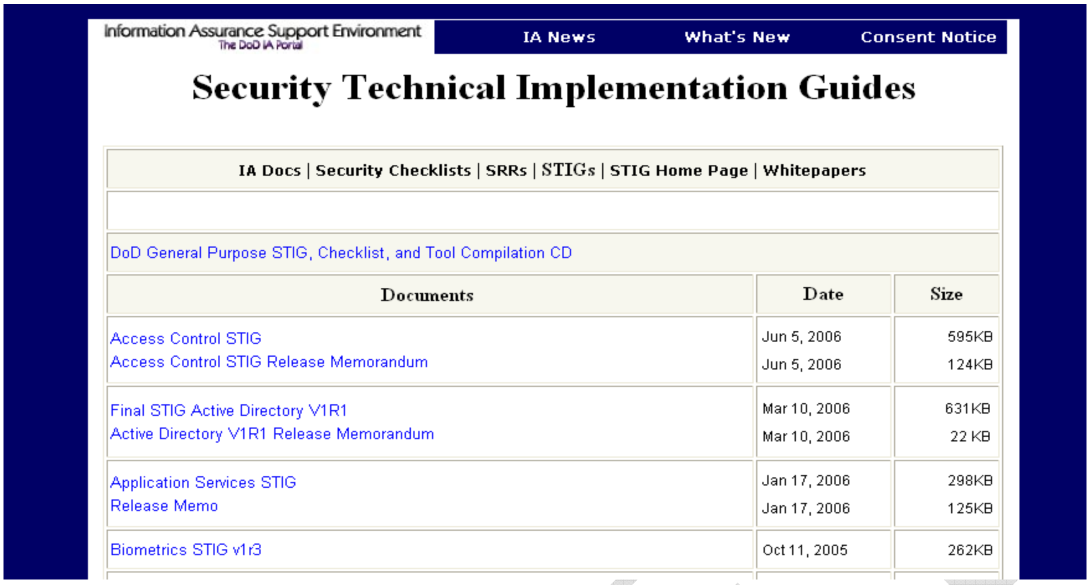
STIG	Description
Enterprise System Management (ESM) STIG	ESM STIG provides security configuration guidance for software products designed to deliver enterprise-class system management functions. While the boundaries of the ESM discipline are such that there is no authoritative definition of an ESM product, Section 2, Enterprise System Management Overview, provides a generic description of the elements characteristic of most ESM products. Section 3, Enterprise System Management Security, provides general guidance for ESM products. Specific commercial products are addressed in appendices.
VMware Enterprise (ESX) Server STIG	ESX Server STIG contains a set of principles and guidelines that serve as the basis for establish VMware ESX Server environments within DoD.
Keyboard, Video, and Mouse (KVM) Switch Checklist	KVM switches are used to connect a single keyboard, video monitor, and mouse to multiple IS, saving space and equipment. They are commonly found in testing laboratories, in server rooms, and with the advent of small inexpensive switches, on desktops to reduce clutter. A/B switches are used by a single peripheral between multiple IS or multiple peripheral devices on a single interface. Switch(es) will refer to both KVM and A/B switches unless otherwise noted.
Instant Messaging Checklist	The instant messaging checklist should be used for enterprise instant messaging systems to collect the data and analysis methodology which will aid the tester with further details in performing the instant messaging checks.
Macintosh STIG	Macintosh STIG provides the technical security policies and a requirement for deploying a secure IS running Macintosh OS X in a DoD Network environment.
.NET Framework Checklist	The .NET Framework checklist targets conditions that weaken the integrity of security, contribute to inefficient security operations and administration. Additionally, the checklist ensures the site has properly installed and implemented the .NET environment and that it is being managed in a way that is secure, efficient, and effective.
Network STIG	Network STIG has been developed to enhance the confidentiality, integrity, and availability of sensitive DoD Automated IA. Each site network/communications infrastructure must provide secure, available, and reliable data for all customers. This document is designed to supplement the security guidance provided by DoD-specific requirements and will assist sites in meeting the minimum requirements, standards, controls, and options required for secure network operations. The intent of this STIG is to include security considerations at the network level needed to provide an acceptable level of risk for information transmitted throughout an enclave.
OS/390 MVS Logical Partition STIG	OS/390 MVS Logical Partition STIG defines the technical criteria necessary to implement MAC II Sensitive functionality within DISA non-classified multiple partitions and classified partitions. This document does not define policy, but it documents the procedures and parameters necessary to implement policy.
OS/390 STIG	OS/390 STIG for most mainframe IA deployed throughout DoD use the IBM OS/390 or z/OS operating system. Controls within OS/390 and z/OS have been developed and documented in IBM references to ensure operating system integrity is maintained. This document is in the process of transitioning from OS/390 to z/OS. Any and all references to OS/390 will apply to both OS/390 and z/OS.
Personal Computer Communications Client STIG	The intent of this STIG is to provide security and implementation considerations that will result in an acceptable level of risk for information located in/on or near the PC/workstation; the information being communicated and the protection of the critical systems that enable and carry the communications.
Sharing Peripherals Across the Network (SPAN) STIG	SPAN STIG provides the technical security policies, requirements, and implementation details for applying security concepts to COTS hardware peripheral devices. For this STIG, peripheral will mean, “any device that allows communication between a system and itself, but is not directly operated by the system.” However, this document does not deal with devices found wholly within the main cabinet of the computer or, with the exception of A/B switches, those devices connected via legacy parallel and serial interfaces.
Secure Remote Computing STIG	Secure Remote Computing STIG provides the technical security policies and requirements for providing a secure remote access environment to users in DoD components. This document discusses both the remote user environment and the network site architecture that supports the remote user. Since information can be stored, processed, or transmitted from a number of locations, IA Systems Management and Information Security must encompass the total environment.
Tandem STIG	Tandem STIG includes security considerations needed to provide an acceptable level of risk for the information that resides on the Tandem systems. The requirements set forth in this document will assist in securing the Tandem NonStop Kernel OS for each site. The Tandem OS includes the Tandem NonStop SQL DB MS, and the Tandem file MS Enscribe.
Unisys STIG	Unisys STIG will define the minimum requirements, standards, controls, options, and procedures that have to be in place for the Unisys Executive and standard system software to meet MAC II sensitive compliance as described in the DoDI 8500.2. Individual sites may implement additional security measures as deemed necessary.

Table B-1. STIG Listing (continued)

STIG	Description
UNIX STIG	Security requirements contained within this STIG are applicable to all DoD administered systems and all systems connected to DoD networks. This document provides requirements and associated steps to limit the security vulnerabilities for a UNIX system. These requirements are designed to assist Security Manager, Information Assurance Manager, Information Assurance Officer, and SA with configuring and maintaining security controls in a UNIX environment. DoD customers use several different UNIX platforms that support different versions of UNIX. All UNIX systems share some common characteristics, but they may implement features differently do not implement all the same features. This document provides security requirements for all common variants of UNIX.
Video Teleconferencing (VTC) STIG	VTC or VC is an extension of traditional telephony technologies, which provide aural communications, with the additional features of visual communications and information sharing. VTC provides simultaneous communications between two or more physical locations enabling the individuals at the various locations to see and hear each other. The visual information sharing capability typically provides the ability for all conferees to see slide presentations, video presentations/movies, and/or hand made drawings on an electronic "whiteboard" generated at one of the locations in the conference.
Virtual Machine/Enterprise Systems Architecture (VM/ESA) STIG	VM/ESA is a multi-access, interactive operating system used in conjunction with the S/390 architecture. VM provides a platform not only for hosting the traditional guest operating systems such as Voice Services Equipment and OS/390, but also for dependent guests such as Multi-User Micro Electrical Machine System Processing System/VM and Advanced IBM UNIX and ESA.
Voice over Internet Protocol (VoIP) STIG	VoIP STIG is published as a tool to assist in securing networks and systems supporting VoIP technology in converging voice and data networks. When applied to DoD networks and systems, this document must be used in conjunction with the DSN STIG, as it contains specific requirements for DoD telecommunications systems and systems connected to the DSN. Additionally, this STIG must be used in conjunction with other STIGs relating to OSs, databases, Web servers, network infrastructure, enclaves, etc., as appropriate.
Web Generic STIG	Web Generic STIG targets conditions that undermine the integrity of security, contribute to inefficient security operations and administration, or may lead to interrupted operations. Additionally, the STIG ensures the site has properly installed and implemented the database environment and that it is being managed in a way that is secure, efficient, and effective. Items on the Web STIG for Internet Information Server are now covered in the DISA Gold Disk V2 and findings will be reported in the relevant Windows portion of this report.
Windows XP 2000/2003 Vista Security Checklist	This is a checklist to Microsoft's Windows 2003 Security Guide and National Security Agency's Guides to Securing Windows 2000 and XP was developed to enhance the confidentiality, integrity, and availability of sensitive DoD Automated Information System using the Windows 2003, 2000, XP and Vista OS. These security settings include those that can be set via the Security Configuration Manager, through Group Policy, as well as manual settings.
Wireless STIG	Wireless STIG is published as a tool to assist in the improving the security of DoD commercial wireless IA. The document is meant to be used in conjunction with the Network STIG and appropriate operating system STIGs.

LEGEND:

A/B	AB Switch	IBM	International Business Machines
AD	Active Directory	IS	Information System
ADAM	Active Directory Application Mode	J2EE	Java^{TM} 2 Platform Enterprise Edition
C2	Command and Control	KVM	Keyboard, Video, and Mouse
CONUS	Continental United States	LAN	Local Area Network
COTS	Commercial Off the Shelf	MAC	Mission Assurance Category
DB	Database	MS	Management System
DISA	Defense Information Systems Agency	OS	Operating System
DNS	Domain Name Server	SPAN	Sharing Peripherals Across the Network
DoD	Department of Defense	SQL	Structured Query Language
DoDI	Department of Defense Instruction	SRR	Security Readiness Review
DRSN	Defense Switch Red Network	STIG	Security Technical Implementation Guidelines
DSN	Defense Switched Network	VM	Virtual Machine
ERP	Enterprise Resource Planning	VoIP	Voice over Internet Protocol
ESA	Enterprise Systems Architecture	VTC	Video Tele-Conferencing
ESM	Enterprise System Management	XP	Experience
IA	Information Assurance		



Security Technical Implementation Guides

IA Docs | Security Checklists | SRRs | STIGs | STIG Home Page | Whitepapers

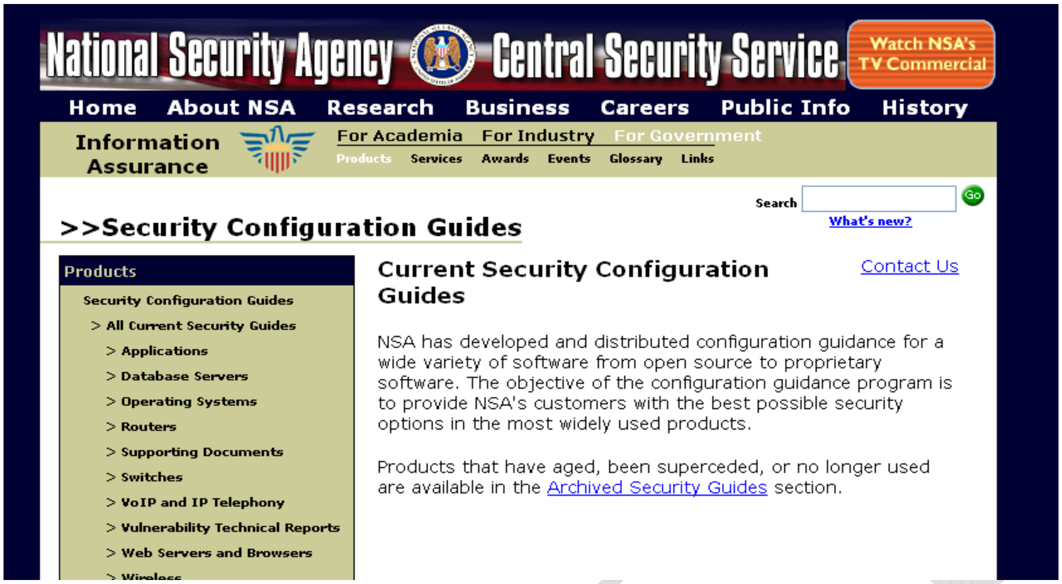
DoD General Purpose STIG, Checklist, and Tool Compilation CD

Documents	Date	Size
Access Control STIG Access Control STIG Release Memorandum	Jun 5, 2006 Jun 5, 2006	595KB 124KB
Final STIG Active Directory V1R1 Active Directory V1R1 Release Memorandum	Mar 10, 2006 Mar 10, 2006	631KB 22 KB
Application Services STIG Release Memo	Jan 17, 2006 Jan 17, 2006	298KB 125KB
Biometrics STIG v1r3	Oct 11, 2005	262KB

Figure B-1. IASE Website

B-2. SECURITY READINESS REVIEW SCRIPTS/GOLD DISK. The DISA Field Security Office (FSO) develops the Gold Disks and Security Readiness Reviews (SRRs) to assist System Administrators (SA) in securing systems and applications in accordance with the DISA STIGs, Checklists, and applicable Center for Internet Security (CIS) benchmarks. This functionality was developed to meet the needs of the system auditors and SA's in accessing the security posture of the respective IS. The SA's, Gold Disks, and SRRs encompass the ability to detect installed products, identify and remediate applicable vulnerabilities, generate a file that is used for asset registration within the vulnerability management system, and provide a findings report.

B-3. NSA OPERATING SYSTEM SECURITY GUIDES/NSA ROUTER AND SWITCH GUIDES. The NSA has written information guides to enhance the posture of both commercial and open source software. These guides cover different version of workstation software, switch software, and router software. The objective of the NSA research program is to develop technological advances and share that information with the software development community through a variety of transfer mechanisms. Figure B-2 provides the documents available at
<http://www.nsa.gov/snac/downloads_all.cfm?MenuID=scg10.3.1>



Current Security Configuration Guides

NSA has developed and distributed configuration guidance for a wide variety of software from open source to proprietary software. The objective of the configuration guidance program is to provide NSA's customers with the best possible security options in the most widely used products.

Products that have aged, been superceded, or no longer used are available in the Archived Security Guides section.

Figure B-2. NSA Website

B-4. MICROSOFT SECURITY GUIDES. Microsoft engineering teams, consultants, support engineers, customers, and partners review and approve Microsoft Security guides. Microsoft worked with consultants and systems engineers, which implemented Windows Server 2003, Windows XP, and Windows 2000 in a variety of environments to establish the latest choice practices to secure these servers and clients. The detailed information guides are available at <http://www.microsoft.com/technet/security/guidance/default.mspx>

B-5. DoDD 8500.1 AND DoDI 8500.2. The DoDD 8500.1 and DoDI 8500.2 establish policy and assign responsibilities to achieve IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology that supports the evolution to network centric warfare. The responsibility of the DoD is crucial to protect and defend information and support information technology. The DoD information is shared across a Global Information Grid that is inherently vulnerable to exploitation and denial of service. The following are contributing factors to vulnerabilities within this grid:

- Increased reliance on commercial information technology and services
- Increased complexity and risk propagation through interconnection
- Extremely rapid pace of technological change
- Distributed and non-standard management structure
- Relatively low cost of entry for adversaries

The DoDI 8500.2, Enclosure 3, establishes fundamental IA requirements for DoD IS in the form of two sets of graded baseline IA Controls. The baseline sets of IA controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels. The IA Controls addressing availability and integrity requirements are tied to the system's MAC based on the importance of the information to the mission, particularly the war fighters' combat mission. Basing the IA Controls addressing confidentiality requirements on the sensitivity or classification of the information ensures a proper security posture. The set of IA Controls applicable to any given DoD information system is always a combination of the IA Controls for its MAC and the IA Controls for its Confidentiality Level.

Achieving baseline IA levels by applying the specified set of IA Controls in a comprehensive IA program includes acquisition, proper security engineering, connection management, and IA administration. An IA Control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA Control are assignable and thus accountable. Table B-2 shows the IA Control subject areas.

Table B-2. IA Control Subject Areas

Abbreviation	Subject Area Name
DC	Security Design and Configuration
IA	Identification and Authentication
EC	Enclave and Computing Environment
EB	Enclave Boundary Defense
PE	Physical and Environmental
PR	Personnel
CO	Continuity
VI	Vulnerability and Incident Management

An IA Control comprises the following:

- Control Subject Area: One of eight groups indicating the major subject or focus area to which an individual IA Control is assigned.
- Control Name: A brief title phrase that describes the individual IA Control.
- Control Text: One or more sentences that describe the IA condition or state that the IA Control is intended to achieve.
- Control Number: A unique identifier comprised of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IA Control Name.

The Joint Interoperability Test Command (JITC) can completely / or thoroughly test only four of the eight IA Control Subject areas because of equipment limitations. The remainder of the IA control subject areas are site specific. The JITC will address DCxx-x, ECxx-x, IAxx-x, and EBxx-x and will partially assess COxx-x and VIxx-x.

DIACAP Scorecard: This is a summary report that shows the certified or accredited implementation status of a DoD Information Systems assigned IA Controls. The scorecard supports or conveys a certification and/or accreditation decision (see Appendix C, Test Preparation Document). The intent of the DIACAP Scorecard is to identify the IA posture of a DoD Information Systems using a format that managers can understand at a glance. After the tester validates the individual IA Controls as compliant, non-compliant, or not applicable, the tester conducts a residual risk analysis (an analysis that determines risk due to partial or unsatisfactory implementation of assigned IA controls). In order to determine the likelihood of a future adverse event, the tester analyzes the threats to a system in conjunction with potential vulnerabilities. The tester also considers the IA Controls that are in place for the system as well as the urgency of completing corrective action. Two indicator codes aid in this analysis: Impact Codes and Severity Codes.

Impact Codes are assigned by the DoD to IA Controls and are maintained through the DIACAP Configuration Control and Management. The impact code for the IA Control is the Technical Advisory Group's assessment of the magnitude of network-wide consequences for a failed IA Control. Within an IA Control Set, the Impact Code indicates each IA Control's relative contribution to the target IA posture, and is expressed as High, Medium, or Low. A High Impact Code is an indicator of greatest impact. Impact Codes listed on the IA Controls detail pages and accessed from within the IA Controls section.

Severity Codes are assigned by the Certifying Authority (CA) to specific findings or deficiencies identified during certification. Severity Codes are an assessment of the likelihood of system-wide IA consequences. The CA assigns the Severity Code to a weakness as part of the certification analysis to indicate risk and to indicate the urgency for corrective action. The Severity Codes are expressed as CAT I, CAT II, and CAT III. The CAT I code is an indicator of the greatest risk and urgency.

The Certification Determination is based on the validation of actual results and an associated risk analysis. It considers Impact Codes associated with IA Controls in a non-compliant status, associated Severity Codes, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate (e.g., dollars, functionality reductions). Certification aids in Plan of Actions and Milestones (POA&M) development and characterizes residual risk.

The JITC scorecard gives organizations the ability to extract test data into the scorecard of their choosing. The scorecard covers the following seven items needed to track IA Controls: IA Control Subject Area, IA Control Number, IA Control Name, Compliant/Non-Compliant, Impact Code, Responsible Entity, and Findings Results Definitions:

- **IA Control Subject Area:** One of eight groups indicating the major subject or focus area to which an individual IA Control is assigned.
- **IA Control Number:** A unique identifier composed of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IA Control Name. The number represents a level of robustness in ascending order that is relative to each IA Control.
- **IA Control Name:** A brief title phrase that describes the individual IA Control.

- **Compliant/Non-Compliant:**
    - **Compliant:** A satisfactory verification of previously agreed to security requirements based on the STIG Checklists.
    - **Non-Compliant:** Failure to meet the recommended security requirements found in the STIG Checklists will result in a Non-Compliant status. Non-Compliant IA Controls will list the checks that require the site to draft a POA&M that describes the corrective actions that will bring their system to a secure state. The findings will show in a dropdown tab (+) on the left of the screen.
- **Impact Code:** Primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system.
- **Responsible Entity:** Used to aid in setting the limits and boundaries identified in testing in a lab environment versus deploying the system to the sponsor's site.
- **Findings Results Definitions:** Below are explanations of terms from the IA STIG and used within the scorecard.
    - **Open:** As applied to the scorecard, an "OPEN" classification in the status column indicates this is a finding for that particular check for that STIG.
    - **Closed:** As applied to the scorecard, a "CLOSED" classification in the status column indicates it may have been originally given an "OPEN" classification in the status but has now been closed.
    - **Fixed On Site (FOS):** As applied to the scorecard, an "FOS" classification in the status column indicates that the vender was able or had the ability to fix or change their system in the JITC lab, to meet the requirement as directed by the STIG.
    - **Not Applicable (NA):** As applied to the scorecard, an "NA" classification in the status column indicates that the requirement given by the STIG check was not relevant to the equipment under test.
    - **Not a Finding (NF):** As applied to the scorecard, an "NF" classification in the status column indicates that as the STIG check is applied to the system, the check is not found to be a finding against the system.
    - **Not Reviewable (NR):** As applied to the scorecard, an "NR" classification in the status column indicates the tester cannot view the check in the STIG (e.g. VxWorks, an Operating System (OS), is oftentimes embedded with a solution that the tester cannot access without a decompiler and a vendor test bench to view).
    - **Required Ancillary Equipment (RAE):** As applied to the scorecard, "RAE" classifications in the status column indicates equipment that has been identified as conditions of fielding when the system is deployed into an operational environment**.** "RAE" is then used in place of an "OPEN" classification in the status column.
    - **To Be Determined (TBD):** As applied to the scorecard, a "TBD" classification in the status column indicates extra information needed before the status can be changed in the scorecard.

Within the delivered scorecard, the following instruction explains how to obtain the corresponding data addressed in the respective acquiring organization's IA Assessment Report.

On the upper-left-hand side of the DIACAP Scorecard, two buttons act as toggle switches that will display or hide information depending on which button is selected. If "1" is selected, it will show only the IA Controls. If "2" is selected, it will show the IA Controls and associated STIG Potential Discrepancy Indicator Requirement Findings, as shown in Figure B-3.

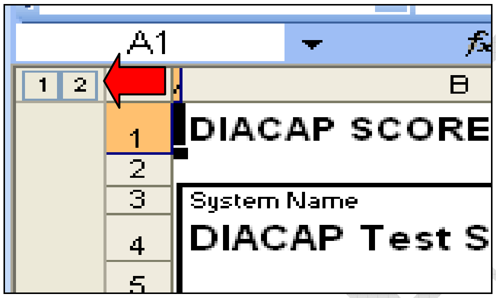


Figure B-3. Toggle Buttons

The scorecard is designed to pull findings from the checklists, associate them to the appropriate IA Controls, and provide access to additional information in the finding notes.

B-6. ADDITIONAL IA REQUIREMENTS. Findings within the Generic Requirements (GR)-815 CORE are no longer used but were cross-matrix with associated STIGs. In addition, findings within those requirements are detailed on the DIACAP Scorecard.

B-7. INTERNET PROTOCOL VERSION 6 (IPv6) REQUIREMENTS. DoD Policy requires most solutions that run on a government network to meet IPv6 requirements. IPv6 requirements are interlaced within many STIGs but also can be found within the UCR2008 document. Table 3 lists appliances and their associated IPv6 requirements which was taken from the UCR2008 document.

Table B-3. IPv6 Rules of Engagement for Products

DSN Product (Appliance)	IPv6 Profile Category	IPv6 Product Rules of Engagement
Multifunction Switch	Simple Server (SS)	MFS in conjunction with the End Instrument must be IPv6 capable
End Office Switch	Simple Server (SS)	EO in conjunction with the End Instrument must be IPv6 capable
Small End Office	Simple Server (SS)	SMEO in conjunction with the End Instrument must be IPv6 Capable
Deployed Voice Exchange	Simple Server (SS)	DVX in conjunction with the End Instrument must be IPv6 Capable
Private Branch Exchange 1	Simple Server (SS)	PBX1 in conjunction with the End Instrument must be IPv6 Capable

Table B-3. IPv6 Rules of Engagement for Products (continued)

DSN Product (Appliance)	IPv6 Profile Category	IPv6 Product Rules of Engagement
Private Branch Exchange 2	Simple Server (SS)	PBX2 in conjunction with the End Instrument must be IPv6 Capable
Customer Premise Equipment	Network Appliance (NA)	Need not be IPv6 capable at this time. Exception: IP End Instruments must be IPv6 capable via Dual Stack or Translation.
Network Element	Network Appliance (NA)	Must be IPv6 capable
LAN Switch	Layer 3 Switch (LS)	Must be Dual Stack IPv6 and IPv4
Router	Router (R)	Must be Dual Stack IPv6 and IPv4
Echo Canceller	Network Appliance (NA)	Need not be IPv6 capable at this time
Integrated Access Switch	Network Appliance (NA)	Must be IPv6 capable via Dual Stack or Translation if supporting an IP end Instrument.
Conference Bridge (external)	Network Appliance (NA)	Need not be IPv6 capable at this time
Multipoint Control Unit	Network Appliance (NA)	Need not be IPv6 capable at this time
Video Telephony Unit	Network Appliance (NA)	Need not be IPv6 capable at this time
H.323/H.320 gateway	Network Appliance (NA)	Need not be IPv6 capable at this time

B-8. INTERNET PROTOCOL VULNERABILITY (IPV). Table B-4 shows the requirements the IPV test team uses to conduct vulnerability scanning and penetration testing. Tools in bold are currently part of the JITC tool chest.

Table B-4. IPV Requirement Tools

Scanning

Amap (Application identification)
Angry IP (port scanner)
Angry IP Scanner (fast host discovery)
Ass (Autonomous system scanner)
Bed.pl (Application fuzzer)
Cheops (Network neighborhood)
Cisco global exploiter (Cisco scanner)
Cisco torch (Cisco oriented scanner)
ExploitTree search (ExploitTree collection)
Grabbb (banner grabber)
GTK-Knocker (Simple GUI portscanner)
Httprint (Webserver fingerprinting)
IKE-Scan (IKE scanner)
Isrscan (Source routed packets scanner)
Knocker (Simple portscanner)
Metasploit (Metasploit command line)
Metasploit (Metasploit console GUI)
Metasploit (Metasploit web interface)
Nbtscan (Netbios scanner)
Nessus (Security scanner)
Netenum (Pingsweep)
Netmask (Requests netmask)
Nikto (Webserver scanner)
Nmap (Network scanner)
NmapFE (Graphical network scanner)
Oreka (record RTP)
Ozyman (DNS tunnel)
Proxychains (Proxifier)
Raccess (Remote scanner)
Retina (Security Scanner)
Scanrand (Stateless scanner)
ScanSSH (SSH identification)
SIP Dump(sniffer/cracker)
SIP scan (scanner)
SIPsniffer (DISA SIP Sniffer)
SiVuS (SIP Vulnerability Scanner)
SiVuS (VoIP scanner)
Smap (scanner)
Smap (SIP scanner)
SMB-Nat (SMB access scanner)
SNMP walk (SNMP analyzer)
SNMP-Fuzzer (SNMP protocol fuzzer)
Stunnel (Universal SSL tunnel)
SuperScan (scanner)
Timestamp (Requests timestamp)
Unicornscan (Fast port scanner)
VoIPong (voice sniffer)
Wikto (Http Scanner)
ZeNMap (port scanner)

Analyzer

Add_registrations (ring two SIP phones)
Authtool (determine user/pw MD5 decode)
Driftnet (Image sniffer)
Dsniff (Password sniffer)
Erase_registration (sends register request to erase)
Etherape (Network monitor)
Ettercap (Sniffer/Interceptor/Logger)
Ethereal (Network sniffer)
Hunt (Sniffer/Interceptor)
IDA Pro (disassembler)
IPTraf (Traffic monitor)
IWAR (war dialer)
Linkbit
Mailsnarf (Mail sniffer)
NetSed (Network edit)
NGrep (Network grep)
Paros (HTTP interception proxy)
Redirectpoison (poisons INVITEs)
Rejhijacker (replaces valid bindings with bogus)
Retina (Security Scanner)
Rtpinject (Inject bogus rtp into stream)
RTPtools (RTP analyzer)
SARA (Security Scanner)
SATAN (Security Scanner)
Sip-kill (sniff INVITES and kill calls)
SIPulator (DISA LCS simulator)
SJPhone (IP phone analyzer)
smbspy (SMB sniffer)
Sniffit (Sniffer)
SSLDump (SSLv3/TLS analyzer)
TcPick (Packet stream editor)
THCScan (war dialer)
udpfloodVLAN (flood dest MAC)
URLsnarf (URL sniffer)
VoIP Hopping (VoIP analyzer)
VOMIT (IP to wave converter)
Wireshark (Network Sniffer)

Table B-4. IPV Requirement Tools (continued)

Spoofing		
Absinthe (SQL injection) Arpoison (an arp poisoner) Arpspoof (ARP spoofer) Burp Proxy (web attack) CAIN (Network sniffer/ARP poisoning) CDP (CDP generator) DHCPX (DHCP flooder) DNSSpoof (DNS spoofer) Etherwake (Generate wake-on-LAN) File2Cable (Traffic replay) Fragroute (Egress rewrite) Fragrouter (IDS evasion toolkit) Hping2 (Packet generator) HSRP (HSRP generator) ICMPRedirect (ICMP redirect packet generator) ICMPUSH (ICMP packet generator) IGRP (IGRP injector)	IRDP (IRDP generator) IRDPresponder (IRDP response generator) Macof (ARP spoofer/generator) NastySIP (packetgenerator) Nemesis-ARP (ARP packet generator) Nemesis-DNS (DNS packet generator) Nemesis-Ethernet (Ethernet packet generator) Nemesis-ICMP (ICMP packet generator) Nemesis-ICMP (ICMP packet generator) Nemesis-IGMP (IGMP generator) Nemesis-IP (IP packet generator) Nemesis-RIP (RIP generator) Nemesis-TCP (TCP packet generator) Nemesis-UDP (UDP traffic generator) Packit (Traffic inject/modify) Packit (Traffic inject/modify) Rpccfg (RPC spoofing)	SendIP (IP packet generator) SIP (packet generator) SIP Bomber (packet generator) SIP_Messenger (create/send SIP msgs) SIP-kill (packet generator) SIPp (packet generator) SIP-redirect (traffic modify) SIPSAK (SIP stress tool) SIPtastic (passive dict attack) SQL Power Injector (SQL injection) SQLNinja (SQL injection) TcPick (Packet stream editor) TcPick (Packet stream editor) TCPReplay (Traffic replay) Trinoo (Denial of Service) Yersinia (Layer 2 protocol injector)
Bruteforce		
ADMsnmp (SNMP bruteforce) Guess-who (SSH bruteforce) Hydra (Multi-purpose bruteforce)	K0ldS (LDAP bruteforce) Obiwan III (HTTP bruteforce) SMB-Nat (SMB access scanner)	TFTP (bruteforce) VNCrack (VNC bruteforce) Xhydra (Graphical bruteforcer)
Password Cracker		
BKHive (SAM recovery) Default password list Fcrackzip (Zip password cracker) John the Ripper (Multi-purpose password cracker)	Lophtcrack (cracker) Nasty (GPG secret key cracker) Rainbowcrack (Hash cracker) Samdump2 (SAM file dumper)	SIPcrack (SIP login dumper/cracker) SIPcrack(sniffer/cracker) Wordlists (Collection of wordlists)
Forensics		
Autopsy (Forensic GUI) OllyDBG (reverse engineering)	Recover (Ext2 file recovery) Testdisk (Partition scanner)	Wipe (Securely delete files)
Fuzzers		
ISIC (IP Stack Integrity Checker)	Protos (H.225, SIP, LDAP Integrity Checker)	WebFuzzer (web checker)

***NOTE:** Current baseline IPV tools are in bold; other IPV tools in this list may be used.

LEGEND:

ADM	Add Drop Multiplexer	LAN	Local Area Network
ARP	Address Resolution Protocol	LCS	Link Command System
Ass	Autonomous system scanner	LDAP	Lightweight Directory Access Protocol
CDP	Computer Data Processing	MAC	Mission Assurance Category
DHCP	Dynamic Host Configuration Protocol	Nmap	Networked Messaging Application Protocol
DISA	Defense Information Systems Agency	RIP	Routing Information Protocol
DNS	Domain Naming Services	RPC	Remote Procedure Call
GPG	GNU Privacy Guard	RTP	Real Time Transport Protocol
GNU	GNU's Not Unix	SAM	Security Accounts Manager
GTK	Gimp Tool Kit (program)	SIP	System Identification Profile
GUI	Graphical User Interface	SMB	Server Message Block
HSRP	Hot Standby Router Protocol	SNMP	Simple Network Messaging Protocol
HTTP	Hypertext Transfer Protocol	SSH	Secure Shell
ICMP	Internet Control Message Protocol	SSLv3	Secure Socket Layer 3
IDS	Intrusion Detection System	TCP	Transmission Control Protocol
IGMP	Internet Group Management Protocol	TFTP	Trivial File Transfer Protocol
IGRP	Internet Gateway Routing Protocol	TLS	Transport Layer Security
IP	Internet Protocol	UDP	Universal Datagram Protocol
IPV	IP Vulnerability	VLAN	Virtual Local Area Network
IRDP	ICMP Router Discovery Protocol	VoIP	Voice over Internet Protocol
ISIC	Internet Protocol Stack Integrity Checker		
IWAR	Integrated Warfare Architecture Requirements		

B-9. PROTOCOL ANALYSIS (PA). Table B-5 shows the requirements the test team uses to conduct generic PA requirements for the APL inclusion as indicated in the requirement. Additional specifications used include those found in American National Standard Institute T1.111 through T1.116. The system is evaluated for its ability to maintain confidentiality, integrity, and availability.

Table B-5. Protocol Analysis Requirement Tools

Analyzer	
Linkbit (IP Analyzer)	Spectra (SS7 Analyzer)
LEGEND: IP Internet Protocol	 SS7 Signaling System 7

APPENDIX C

TEST PREPARATION DOCUMENT

The Information Assurance Test Team (IATT) uses the Test Preparation document to record information relevant to the System Under Test (SUT). The information recorded is detailed component information, including manufacturer, make, and model, operating system, vendor-developed software, other commercial software, version, and firmware. The IATT tracks the date of the test, tracking number of the SUT, tester's name, vendor's name, vendor's solution name, e-mail addresses, and phone numbers. The document is signed by the vendor and the lead tester for each phase of testing.

DSN IA Test Team Test Preparation Document

Tracking Number: ____________________________

Vendor Information	
Vendor Name	
Name of SUT	
Type of System	MFS □ SMEO □ EO □ NE □ CPE □ NMS □
	ASLAN □ ECAN □ PBX □ Other □ List:
Vendor POC	
Email	
Phone	

Testing Dates		
Phase I		Complete □
Phase II		Complete □
Phase III		Complete □
IO Testing		Complete □

Tester Information		
Phase I Tester (STIG)	Name	
	Phone	
	Email	
Phase II Tester (IPV)	Name	
	Phone	
	Email	
Phase III Tester (PA/TDM)	Name	
	Phone	
	Email	

System Information		
STIG Test	Functionality	
	Before Testing □ YES □ NO	After Testing □ YES □ NO
IPV Test	Functionality	
	Before Testing □ YES □ NO	After Testing □ YES □ NO
PA/TDM Test	Functionality	
	Before Testing □ YES □ NO	After Testing □ YES □ NO

DSN IA Test Team Test Preparation Document
Tracking Number: ______________________________

System Information			
System Diagram (Copy to "T" Drive see note)	Attached □ YES □ NO	Drawing Type	Visio □ Jpeg □ PowerPoint □
System and component description attached? □ YES □ NO			
In-brief minutes attached? □ YES □ NO			
Location GNTF □ GNTF ANNEX □	Circle on Map and note rack numbers below		
RAE Equipment connections	RADIUS □ SysLog □ AD □ TACACS □ Client □		

IP Information			
DHCP in use □ DHCP capable □			
IP Address Start	IP Address End	Subnet	VLANs
Routers in use □	Configurations collected □		
Switches in use □	Configurations collected □		
NOTE: Store information on "T" Drive under IA Program			

Adjust as needed top portion with the correct switches and versions.
Use this table to build the "Table 5" on the report; this can be adjusted as needed.

System Name	Hardware/Software Release		
Required Ancillary Equipment	Public Key Infrastructure		
	Remote Authentication Dial-In User Server		
	SysLog Server		
	Active Directory		
System Name (from the initial contact meeting minutes)	**Hardware**	**Card Name**	**Software/ Firmware**
		Part Number/Name	
SUT Telephones			
Telephone type	**Model**	**Firmware**	
Analog/ISDN/IP			

LEGEND:
IP Internet Protocol
ISDN Integrated Services Digital Network
SUT System Under Test

Note: Put in logical order and ensure information is complete; if there are no cards/part numbers/etc., remove that information from this table before completing the report.

DSN IA Test Team Test Preparation Document
Tracking Number: ______________________

By signing this document, I have verified that all information is identified correctly and all version numbers identified within this document have been physically verified on the system under test.

_______________________________ DATE: _____________
Vendor

_______________________________ DATE: _____________
STIG Tester

_______________________________ DATE: _____________
IPV Tester

_______________________________ DATE: _____________
PA/TDM Tester

_______________________________ DATE: _____________
IO Tester

_______________________________ DATE: _____________
STIG Technical Lead (Gardner)

_______________________________ DATE: _____________
IPV Technical Lead (Searle)

Have the passwords been turned over to the GNTF System Administrator:
□ **YES** □ **NO** (check one)

_______________________________ DATE: _____________
GNTF System Administrator

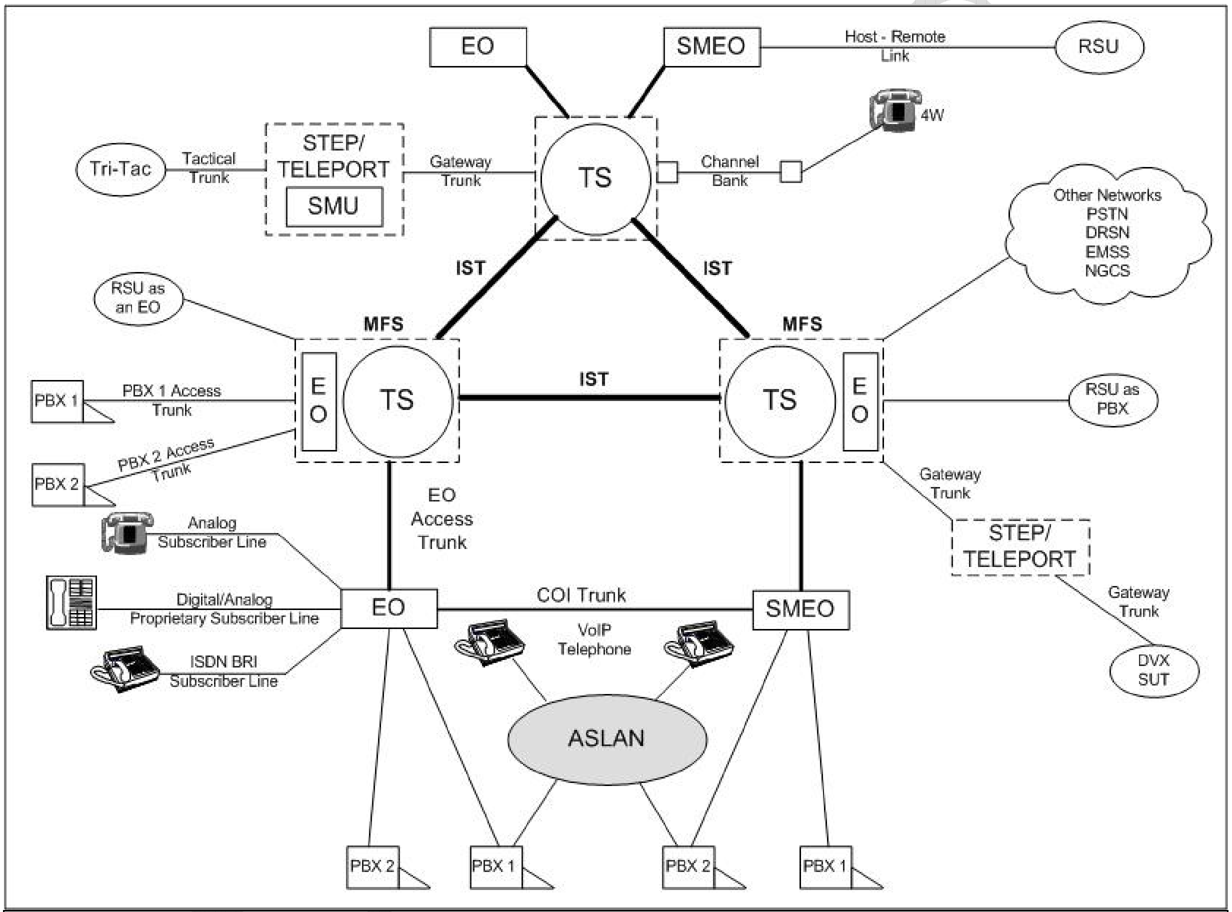
****NOTE: Turn over all required documents (this document, copies of relevant results, etc.) to the next tester(s). Place original test preparation document in designated storage area. ALL testers must coordinate with the GNTF SA for any administrator access to ANY equipment**

(The page intentionally left blank.)

APPENDIX D

DSN ARCHITECTURE

The Defense Switched Network (DSN) architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Each Information Assurance findings report will include the system as shown in Figure D-1 and is annotated by the System Under Test.



LEGEND:

4W	4 Wire	NATO	North Atlantic Treaty Organization
ASLAN	Assured Services Local Area Network	NGCS	NATO General Purpose Segment Communication System
BRI	Basic Rate Interface		
CB	Channel Bank	PBX 1	Private Branch Exchange 1
COI	Community of Interest	PBX 2	Private Branch Exchange 2
DRSN	Defense Red Switch Network	PSTN	Public Switched Telephone Network
DSN	Defense Switched Network	RSU	Remote Switching Unit
DVX	Deployable Voice Exchange	SMEO	Small End Office
EO	End Office	SMU	Switch Multiplexer Unit
EMSS	Enhanced Mobile Satellite Services	STEP	Standardized Tactical Entry Point
ISDN	Integrated Services Digital Network	Tri-Tac	Tri-Service Tactical Communications Program
IST	Inter-Switch Trunk	TS	Tandem Switch
MFS	Multi-Function Switch		

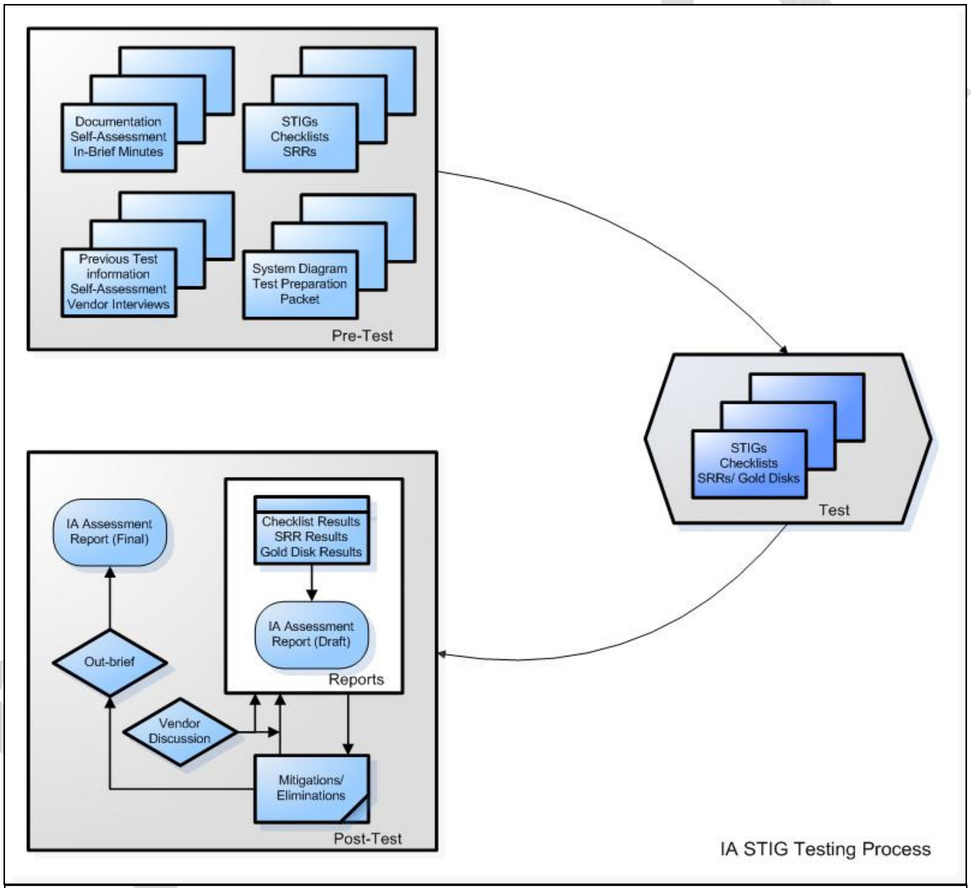
Figure D-1. DSN Architecture

(This page intentionally left blank.)

APPENDIX E

ASSESSMENT OBJECTIVES, CRITERIA, PROCEDURES AND DATA REQUIRED

The following sections outline the objectives, criteria, procedures, and data required for the Information Assurance (IA) assessment of a System Under Test (SUT). An IA assessment is required before consideration of a SUT for inclusion on the Defense Switched Network (DSN) Unified Capabilities Approved Products List (APL). The process is divided into three phases, as shown in Figure E-1: Pre-Test, Test, and Post-Test.



LEGEND:

IA	Information Assurance	STIG	Security Technical Implementation Guidelines
SRR	Security Readiness Review		

Figure E-1. IA STIG Testing Process

E-1. STIG TESTING PROCEDURES.

1. Pre-Test.

a. Information Collection. This section describes the necessary documents needed to conduct an IA assessment of a SUT. The documents are also used for special case assessments of an SUT.

(1) Vendor Documentation. Vendors are required to submit documentation during the initial APL certification process. Documentation includes:

- Network diagrams
- System descriptions
- User guides
- Administration and technical manuals
- White papers

Other requirements include detailed information about each component such as name, model number, software and/or applications applied and version number of software and/or applications. The information is critical to ensure an accurate assessment of the SUT.

(2) Previous Test Cases. During an out-brief, issues may be brought to the table that would initiate a Verification and Validation (V&V) test. A V&V is required if the vendor has mitigation(s) that could be corrected during a short period of time, at the request of a representative from the Field Security Office (FSO), or if problems such as potential vulnerabilities were identified during other phases of testing.

b. In-Briefs. In-briefs are conducted after the APL bundle has been submitted and all items required have been verified by the DSN-Unified Capabilities Connection Office (UCCO). Participates include a representative from the FSO, sponsor, a vendor representative and the IA Test Team (IATT) team lead. Initial contact minutes are drafted, which will detail what Security Technical Information Guidelines (STIG) documents to use, what Required Ancillary Equipment (RAE) devices are required, if any, and other test details.

c. Self-Assessments. Vendors are required to conduct a self-assessment of their solution to ascertain the security posture before the system is brought to test. The vendor will apply the exact same STIGs that will be applied to the actual test.

d. Reference Materials. The following section provides a description of references that are used when performing an IA assessment.

(1) STIGs/Checklists. STIGs are based on Best Business Practices, Department of Defense Directives (DoDD), other Department of Defense (DoD) publications and instruction, Public Laws, and other Federal Government regulations. The STIGs provided detailed instructions on how to secure and establish a baseline security posture for a DoD information system. Checklists used in conjunction with the parent

STIG. Not all checklists have parents STIGs. STIGs and checklists can be assessed at the following respective links: <http://iase.disa.mil/stigs/stig/index.html> <http://iase.disa.mil/stigs/checklist/index.html>.

(2) Security Readiness Reviews (SRR)/Gold Disks. The Defense Information Systems Agency (DISA) Gold Disks and SRRs are automated tools and scripts used to test a system's security posture against DISA established baselines. The SRRs and Gold Disks can be found at the following link: <http://iase.disa.mil/stigs/SRR/index.html>.

(3) Network Diagrams. The network diagram details all components of the SUT in its test configuration. The test configuration is how the system will be deployed. The diagram will be checked against actual test configuration in the lab environment before testing will commence. If any changes are required, the changes will be agreed upon by the Action Officer, vendor, and tester(s) before the diagram is re-submitted to the DSN-UCCO.

2. Test. Testing evaluates the security readiness of the system against the DISA minimum security baseline. The first day of testing will consist of:

- Vendor and tester will discuss the concept of the system and conduct a functionality test
- Network diagram will be validated; if additional components are noted, additional STIGs may be added
- Tester ensures test boundaries are stated and understood
- The tester informs the vendor that during the test, time will be set aside for a meeting with the government if desired, to answer questions regarding the test and APL process, and address vendor concerns.

During the mid-week of testing, a vendor status meeting is scheduled to discuss testing at that point and any issue the vendor or tester has will be addressed. Participants include the sponsor, Action Officer, vendors, and testers.

a. Defense Switched Network (DSN) IATT Test Preparation Document. This document is used to record pertinent test data. Information recorded includes: detailed component information, Internet Protocol (IP) address, vendor and tester contact information, dates and place of testing (Global Information Grid Network Test Facility (GTNF) or GTNF annex), and other important information to assist in tracking progress of testing.

b. Network Diagram. The network diagram details all components of the SUT in its test configuration. The test configuration is how the system will be deployed. The diagram will be checked against actual test configuration in the lab environment before testing will commence. If any changes are required, the changes will be agreed upon by the Action Officer, vendor, and tester(s) before the diagram is re-submitted to the DSN-UCCO.

c. Securing the Management Workstation/Console. System configuration will often include a management workstation or console. This component is often used to access the primary component of the test configuration, although, there are several options for an OS such as UNIX, LINUX, or Mac. This section will detail security settings required that deviated from what is documented in the Windows Experience (XP) STIG. Each application that is installed introduces additional vulnerabilities to the workstation and the entire system. This procedure is intended for un-partitioned hard disk drives.

(1) Windows XP Professional Installation.

(a) All partitions must be configured as New Technology File System (NTFS) unless otherwise needed for images or other small storage requirements. Hard disk drives will have no un-partitioned space

(b) Save and, remove all data; perform a clean install.

(c) Install the latest service pack.

(d) Install Java Runtime Environment, if required.

(e) Install all Windows updates and device drivers.

(f) Disable excessive devices in the systems' Basic Input/Output System (BIOS).

(2) Anti-Virus.

(a) Install and update an anti-virus tool—McAfee or Symantec.

(b) Configure weekly full scans and daily quick scans. (See the Desktop Application Checklist for procedures.)

(3) POSIX Subsystem File Components.

(a) Select the "Search" button from the Tools bar and enter the following in the "Search for files and folders named" field: POSIX, PSX, select search.

(b) If the search returns any of the following files, delete them: "POSIX.EXE," "PSXSS.EXE" or "PSXDLL.DLL."

(4) Securing Event Logs. Reference Windows 2003/XP/2000/VISTA Addendum for details on how to secure the event logs. When an event log is cleared, the system deletes and recreates the log file. This, in effect, restores the default file permissions to those of the parent directory. Permissions for the "Auditors" group are removed and the Administrators group receives full control. Follow the procedures below to prevent the problem of resetting permissions on the event log:

(a) Create a subdirectory for the event logs: SystemRoot%\system32\config\EventLogs.

(b) Set Access Control Lists (ACL) permissions on this directory. (Auditors – Full Control, System - Full Control, Administrators – Read).

(c) Copy the event logs from the \config directory to the new EventLogs directory.

(d) Edit the Registry using regedit.exe.

(e) Expand the following key:

HKLM\SYSTEM\CurrentControlSet\Services\EventLog.

(f) Select the Application key and double click the “File” value.

(g) Change the string value to: %SystemRoot%\system32\config\EventLogs\Appevent.evt.

(h) Repeat steps e-g for setting the registry keys for “Security (Secevent.evt)” and “System (Sysevent.evt)”.

(5) Password Filter. Reference the Windows XP Checklist Section 5 for details. JTF-GNO Communications Tasking Order (CTO) 07-015, states: Passwords will contain a mix of at least two lowercase letters, two uppercase letters, two numbers, and two special characters. The password will be a minimum of 14 characters in length. NOTE: Enpasflt.dll included with the Gold Disk will enforce these requirements. It can be found on Compact Disk 1 in the Install\Misc directory. Installation Instructions:

(a) Copy and paste the Enpasflt.dll file in: %systemroot%\system32.

(b) Restart the system; registry key “HKLM\System\CurrentControlSet\Control\LSA\Notification Packages” must include “enpasflt”.

(c) Disable Microsoft Password Complexity (5.4.1.5). Set policy “Password must meet complexity requirements” to Disabled.

NOTE: Several system-generated user accounts may generate findings in an SRR, stating the account is not required to have a password (i.e., IUSR_…, TSUser). To correct this problem, enter the following on a command line: “Net user <account_name> /passwordreq:yes”.

(6) Using the Microsoft Management Console (MMC). Reference Windows XP checklist Section 5 for details. The MMC is the primary system configuration tool for Windows XP. It uses “snap-in” functions to configure various areas of the system. The security configuration and analysis snap-in permits the analysis of account policy, system auditing, local policies, event logs, services, registry ACLs and auditing, and file ACLs and auditing. See Figure E-2.

(a) Procedure: To use MMC and load the Security Configuration and Analysis snap-in:

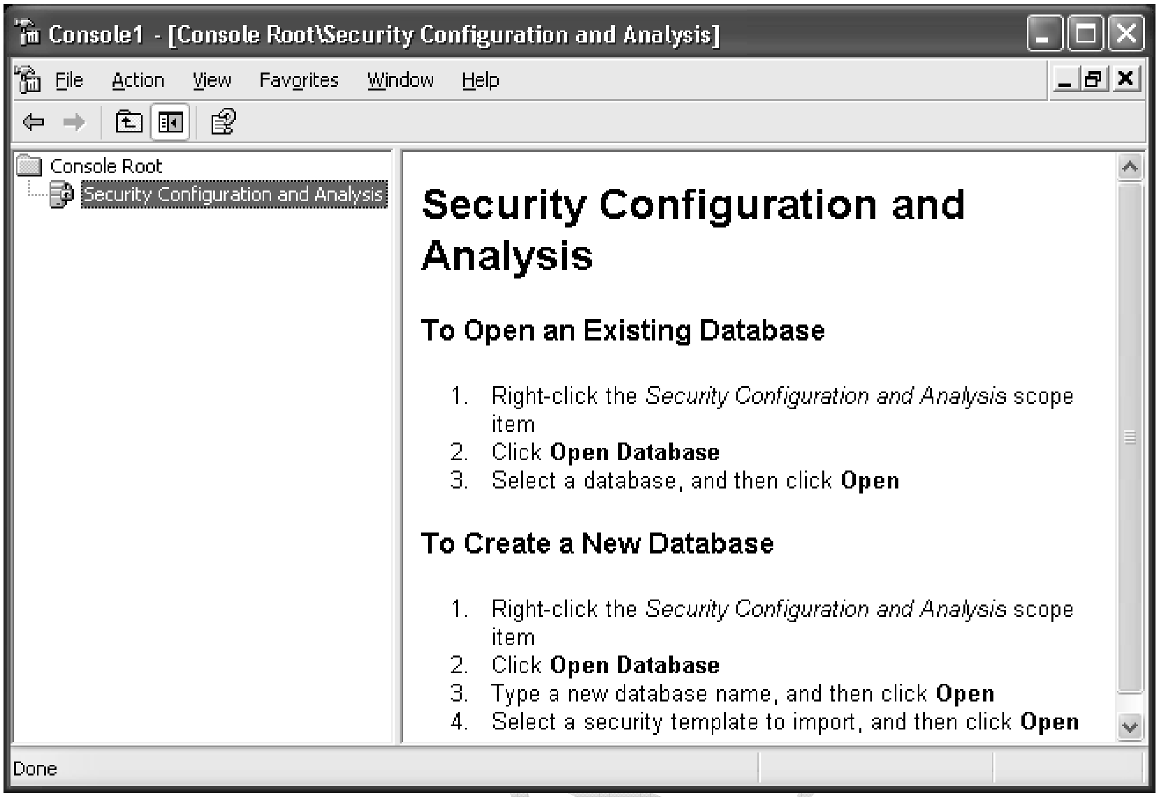
1. Select Start and Run, and type mmc.exe in the Run dialog box.

2. Select “File” from the MMC menu bar.

4. Select “Add/Remove snap-in” from the drop-down menu.

5. Click the “Add” button on the Standalone tab.

6. Select the “Security Configuration and Analysis” snap-in and click the “Add” button, Close, and OK.


Console1 - [Console Root\Security Configuration and Analysis]
File
Action
View
Favorites
Window
Help
Console Root
Security Configuration and Analysis
Done

Security Configuration and Analysis

To Open an Existing Database

1. Right-click the *Security Configuration and Analysis* scope item
2. Click **Open Database**
3. Select a database, and then click **Open**

To Create a New Database

1. Right-click the *Security Configuration and Analysis* scope item
2. Click **Open Database**
3. Type a new database name, and then click **Open**
4. Select a security template to import, and then click **Open**

Figure E-2. Security Configuration and Analysis

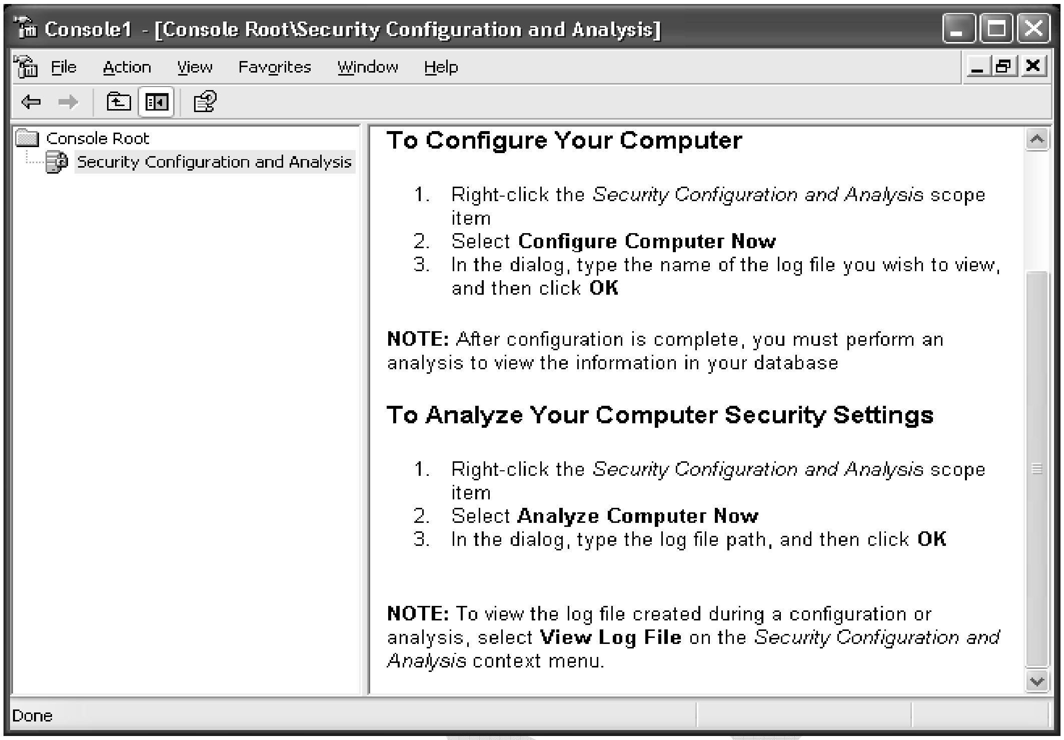
(b) Use the following procedure with the Security Configuration and Analysis snap-in and Figure E-3 to prepare the files for analyzing the system:

1. Right-click on the Security Configuration and Analysis object in the left window, Select ‘Open Database’.

2. Enter “C:\temp\scan\srr.sdb” for the database name.

4. In the ‘Import Template’ window enter the appropriate file name for a workstation (i.e., Hardening.inf).

5. Check the box to “Clear the database before importing.” Select “Open.”


Console1 - [Console Root\Security Configuration and Analysis]
File
Action
View
Favorites
Window
Help
Console Root
Security Configuration and Analysis
Done

To Configure Your Computer

1. Right-click the *Security Configuration and Analysis* scope item
2. Select **Configure Computer Now**
3. In the dialog, type the name of the log file you wish to view, and then click **OK**

NOTE: After configuration is complete, you must perform an analysis to view the information in your database

To Analyze Your Computer Security Settings

1. Right-click the *Security Configuration and Analysis* scope item
2. Select **Analyze Computer Now**
3. In the dialog, type the log file path, and then click **OK**

NOTE: To view the log file created during a configuration or analysis, select **View Log File** on the *Security Configuration and Analysis* context menu.

Figure E-3. Configure Your Computer

(c) Use the following procedure to analyze the system:

1. Right-click on the Security Configuration and Analysis object in the left window.

2. Select “Analyze Computer Now.”

3. Enter “C:\temp\scan\srr.log” for the log name in the ‘Error log file path’ window and click OK. Figure E-4 shows the window that will display.

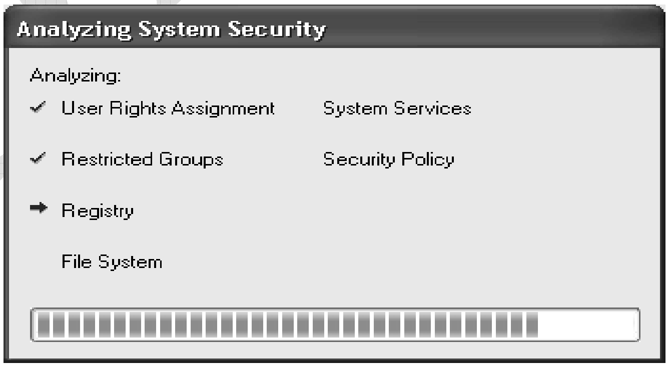
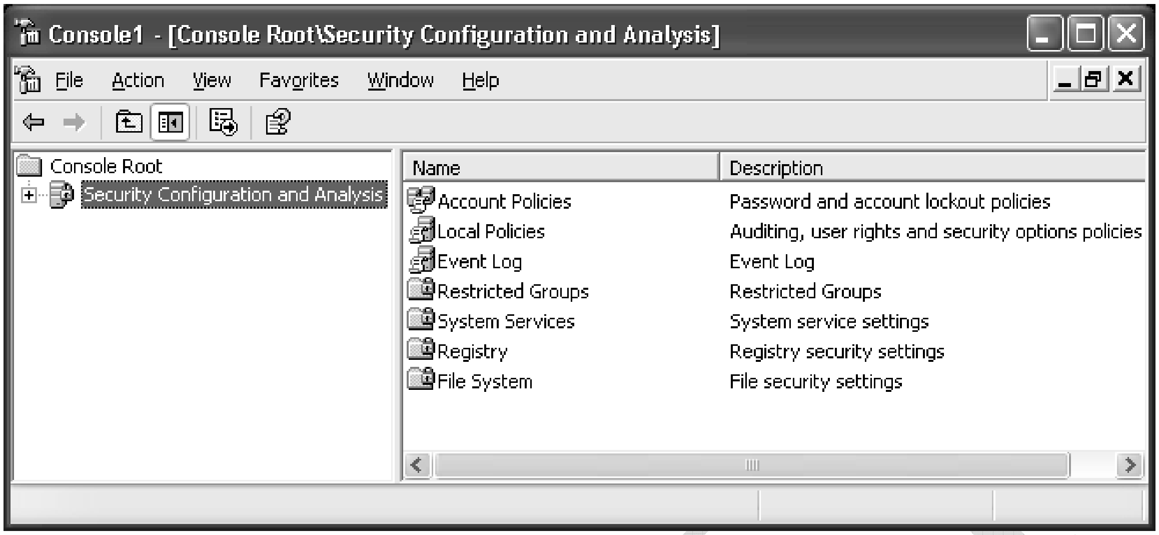


Figure E-4. Analyzing System Security

4. When the analysis is completed, the right pane will show the analysis objects. See Figure E-5.


Console1 - [Console Root\Security Configuration and Analysis]
File
Action
View
Favorites
Window
Help
Console Root
Security Configuration and Analysis

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings

Figure E-5. Analysis Objects

5. To configure your computer:

a. Right-click on the Security Configuration and Analysis object in the left window.

b. Select “Configure Computer Now.”

c. Enter “C:\temp\scan\srr.log” for the log name in the ‘Error log file path’ window and click OK; reboot the workstation.

d. Securing the Workstation/Console using the Gold Disks. Ensure the workstation meets the minimum requirements as outlined in Table E-1. Follow the procedures outlined in Appendix E, Table E-2. Results will be imported into the Defense Information Assurance Certification and Accreditation Process (DIACAP) Scorecard.

(1) Gold Disk After Results.

(a) Log into the workstation and ensure Windows functionality.

(b) Follow the procedures outlined in Appendix E, Table E-2, to use the Gold Disk and verify the security settings.

(c) Record the results of the Gold Disk scan as the after results and import into the DIACAP Scorecard using the Gold Disk import script.

Table E-3 displays the DISA Gold Disk test procedures alternate with out an optical drive. Table E-4 displays the DISA Gold Disk test procedures with alternate command line. Table E-5 details that SRR test procedures for UNIX.

Table E-1. Gold Disk Minimum System Requirements

Gold Disk Minimum System Requirements	
Operating System	Windows 2000 Professional Windows 2000 Member Server Windows 2000 Domain Controller Windows 2003 Member Server Windows 2003 Domain Controller Windows XP
Internet Explorer	Internet Explorer 6.0 or above
Account Privileges	User account used to run the Gold Disk must have Administrator privileges.
User Right	User account used to run the Gold Disk must have "Manage Auditing and Security Log"
Minimum Screen Resolution	800 x 600
LEGEND: XP Experience	

Table E-2. DISA Gold Disk Test Procedures

DISA Gold Disk Test Procedures	
Objective	To determine if the System Under Test is compliant with the Defense Information Systems Agency security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Gold Disk is the most current version available. 2. Review the Gold Disk user guide to verify any changes to procedure for running the Gold Disk. 3. Perform a full functionality test. 4. Ensure Internet Explorer 6 is installed and fully functional prior to execution of the Gold Disk. 5. Determine the applicable procedure to be used based on system configuration. 6. Create a folder for temporary collection for computer generated reports in an easily accessible place. 7. Insert the Gold Compact Disk into an available optical drive. 8. Using Windows Explorer, double-click on the file "Launcher.exe". 9. After the pre-scan is completed the following items must be selected for each asset listed in the "Asset Posture" window: • I – Mission Critical • Sensitive • Platinum 10. Select the "Evaluate Asset" button from the tool bar. 11. After evaluation is completed save a preliminarily report to the temporary folder that was created in step 6. • Click Reports tab on the file toolbar. • Select Vulnerability Management System (VMS) 6.X. • Save the file as VMS 6.X before.xml 12. Evaluate all items listed for potential vulnerabilities and false positives. 13. If time permits, the vendor may remediate any findings that are marked as open. 14. Evaluate all findings marked as unknown. If time permits, the vendor may remediate these findings. 15. Click Reports tab on the file toolbar. 16. Select VMS 6.X. 17. Save a final report with a different name to the temporary folder that was created in step 6. See section E-1.3.1 for instructions on reading the Extensible Markup Language file. 18. Perform a full functionality test.
Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable

Table E-2. DISA Gold Disk Test Procedures (continued)

DISA Gold Disk Test Procedures (continued)	
Data Required (continued)	**Data:** • VMS Identification Number • Potential Discrepancy Indicator • Number finding that resulted in errors • IA Control information
Collection Forms	Information Assurance Assessment Report. DIACAP Scorecard
LEGEND: DIACAP DoD Information Assurance Certification and Accreditation Process DoD Department of Defense DISA Defense Information Systems Agency	IA Information Assurance VMS Vulnerability Management System

Table E-3. DISA Gold Disk Test Procedures: Alternate No Optical Drive

DISA Gold Disk Test Procedures: Alternate no Optical Drive	
Objective	To determine if the System Under Test is compliant with the Defense Information Systems Agency security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Gold Disk is the most current version available. 2. Review the Gold Disk user guide to verify any changes to procedure for running the Gold Disk. 3. Perform a full functionality test. 4. Ensure Internet Explorer 6 is installed and fully functional prior to the execution of the Gold Disk. 5. Determine the applicable procedure to be used based on system configuration. 6. Create a folder for temporary collection of computer-generated reports in an easily accessible place. Insert the Gold Compact Disk into an available optical drive on separate machine.
Procedures	7. Either copies content of the Gold Disk, to test system or to a portable Universal Serial Bus (USB) drive (USB Drive must have more than 512 Megabyte of free space). 8. Using Windows Explorer double-click on the file “Launcher.exe.” 9. After the pre-scan is complete the following items must be selected for each asset listed in the “Asset Posture” window • I – Mission Critical • Sensitive • Platinum 11. Select the “Evaluate Asset” button from the tool bar. 12. After evaluation is complete save a preliminarily report to the temporary folder that was created in step 6: • Click Reports tab on the file toolbar. • Select Vulnerability Management System (VMS) 6.X. • Save the file as VMS-6xbefore. 13. Evaluate all items listed for potential vulnerabilities and false positives. 14. If time permits the vendor may remediate any findings that are marked as open. 15. Evaluate all findings marked as unknown; if time permits the vendor may remediate these findings. 16. Save a final report, with a different name, to the temporary folder that was created in step 6. See section E-1.3.1 for instructions on reading the Extensible Markup Language file. 17. Perform a full functionality test.
Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable Data: • VMS Identification Number • Potential Discrepancy Indicator • Number finding that resulted in errors • IA Control information

Table E-3. DISA Gold Disk Test Procedures: Alternate No Optical Drive (continued)

DISA Gold Disk Test Procedures: Alternate no Optical Drive	
Collection Form	Information Assurance Assessment Report. DIACAP Scorecard

LEGEND:

DIACAP	DoD Information Assurance Certification and Accreditation Process	IA	Information Assurance
DoD	Department of Defense	USB	Universal Serial Bus
DISA	Defense Information Systems Agency	VMS	Vulnerability Management System

Table E-4. DISA Gold Disk Test Procedures: Alternate Command Line

DISA Gold Disk Test Procedures: Alternate Command Line	
Objective	To determine if the System Under Test is compliant with the Defense Information Systems Agency security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Gold Disk is the most current version available. 2. Review the Gold Disk user guide to verify any changes to procedure for running the Gold Disk. 3. Perform a full functionality test. 4. Ensure Internet Explorer 6 is installed and fully functional prior to the execution of the Gold Disk. 5. Determine the applicable procedure to be used based on system configuration. 6. Create a folder for temporary collection of computer-generated reports in an easily accessible place. 7. Insert the Gold Compact Disk into an available optical drive. 8. The command line option for non-interactive mode is "pgd.exe /f:<path:filename>", where "<path:filename>" is replaced by the full path and filename of the non-interactive run control file. 9. The Non-Interactive Control File you must specify all of these options: • MAC • Confidentiality • Report Path • Report Filename • Report Format(s) • Whether to create an asset Extensible Markup Language (XML) file (TRUE/FALSE) • Target(s) o Target Identification (ID) Number o Policy ID Number o Whether to perform fixing (TRUE/FALSE) 10. Any vulnerabilities for which fixing should be skipped for this target (Using the Vulnerability ID(s)). 11. Save a final report, with a different name, to the temporary folder that was created in step 6. See section E-1.3.1 for instructions on reading the XML file. 12. Perform a full functionality test.
Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable Data: • VMS Identification Number • Potential Discrepancy Indicator • Number finding that resulted in errors • IA Control information
Collection Form	Information Assurance Assessment Report. DIACAP Scorecard

LEGEND:

DIACAP	DoD Information Assurance Certification and Accreditation Process	IA	Information Assurance
		ID	Identification
		MAC	Mission Assurance Category
DISA	Defense Information Systems Agency	VMS	Vulnerability Management System
DoD	Department of Defense	XML	Extensible Markup Language

Table E-5. SRR Test Procedures: UNIX

SRR Test Procedures: UNIX	
Objective	To determine if the System Under Test is compliant with the Defense Information Systems Agency security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Security Technical Implementation Guide and SRR to be used are the most current version being used. 2. Perform a full functionality test. 3. The tester will ensure a means of logging onto the system as root (using su -) has been established for conducting the SRR. 4. Load and untar the scripts in a directory tree which will not interfere with the actual SRR, i.e., not in somebody's home directory tree. Some suggestions are: • /export/home/SRR, for Solaris • /home/SRR for Hewlett Packard-UNIX (HP-UX) 5. Use a directory tree where there is a lot of available space (determined by using df -k on Solaris (and others), and bdf on HP. 6. The SRR directory will be used to transfer the UNIX Scripts, which conducts the SRR to build the output data from (hostname.tar.Z). 7. Always ensure file transfers are accomplished using the binary file transfer mode of the data transfer utility. 8. After transferring the script tar file to the machine, the reviewer will execute su -, and the vendor will enter the root password. • Ensure the root SHELL is /sbin/sh. 9. Ensure the account/directory established for the SRR is located in a sizeable file system that is NOT one of /, /etc, /var, /usr/bin, /usr/sbin, /sbin or any other level file system. A user file system with adequate space is appropriate. Adequate space is 50 megbytes or more. Ensure permission on the account/directory into which the scripts are transferred is 700 and the permission of the script tar file is 700. Check file system space using the following command: • df (for Solaris) or bdf (for HP-UX) 10. Uncompress the tar file using one of the following commands. (NOTE: Ensure the name of SRR file is typed EXACTLY as the one transferred remember case sensitivity.) uncompress ddmmmyy-Unix.tar.Z • gunzip ddmmmyy-Unix.tar.gz • unzip ddmmmyy-Unix.tar.zip • bzip2 -d ddmmmyy-Unix.tar.bz2 NOTE: If there is an error reading the file, it usually means the file was NOT transferred using the binary command. 11. Extract the tar file. This process will create a directory named Script in the SRR directory and that directory will contain all the Script subdirectories and data. Make sure you are in the SRR directory. Extract the scripts using the following command: • tar xvf ddmmmyy-Unix.tar NOTE: If there is an error, such as "checksum error", it usually means the tar file was NOT transferred using the binary option. 12. Change directory to the newly created Script directory using the following command: • cd Script.Month 13. The scripts can now be applied using one of the following commands: • Use nohup /Start-SRR & (if running the scripts in background and using nohup to create a record of all the actions in the nohup.out file). This command will also run the utilities for crack and the global find. It will not take the "Tivoli" option, which would run the scripts and create an output report for installations performing self-assessments using the Tivoli Distribution function to distribute the scripts, execute the scripts, and retrieve the output of the scripts into a home grown reporting facility) • Use ./Start-SRR & (to just run the scripts in background without the nohup.out file and with all the other options listed above) • Use ./Start-SRR nocrack (may also be used with nohup and in background will run the SRR scripts but skip running crack, which can take hours to execute on a large system). • Use ./Start-SRR tivoli (may also be used with nohup, in background and in combination with nocrack will simply run the scripts and generate a report file for transfer back to the master Tivoli console).

Table E-5. SRR Test Procedures: UNIX (continued)

SRR Test Procedures	
Procedures (continued)	• Use ./Start-SRR nofind (may be used in combination with any or all of nocrack and tivoli. The nofind option bypasses the execution of the global find that may be useful if re-running numerous scripts that do not use the output of the global find). • The defaults for the options for Start-SRR are: nocrack=y (run crack) nofind=y (run the global find) Tivoli=n (do not produce Tivoli output) 14. Outputs from running the scripts will include (NOTE: Item Number = Checklist Item Number = Potential Discrepancy Indicator (PDI) Number (or, Secure Digital Identification) = Script number): • Hostname: Directory created under the Script directory where the following output files are stored: • PDI.Result: A file for each script containing finding status, description, and examples (if status is Open, Not Reviewed, or Not Applicable). • PDI.Examples: A file containing the full list of findings for an item. It will only exist if there have been findings, if the item is a manual review item or, it is not applicable to the operating system/machine type. • Hostname.Log: A file created for each item. It will contain error messages if the script failed or, it will be size zero. • SRR.Initial.Results: A file containing a summary list of PDIs marked as Not Reviewed; Counts of findings in all categories; PDIs marked as Open findings; PDIs marked as Not a Finding; Scripts which did not complete (if any); Scripts which found Category I Findings (if any). • Hostname.patch.report: For Solaris systems, a file that contains a detailed patch report for the reviewed Solaris system. The system must have perl 5.005 in the search PATH or it will not be produced. Otherwise, the manual side will run and all the results will be in the G033.Examples file. • FindFile: A file containing the results of the global find run at the beginning of the SRR from Start-SRR. Hostname.txt: A file created by the Security Readiness Review Data Base (SRRDB) update program for import into the SRR database. SiteConfiguration: Directory, containing copies of several configuration files, to be used by the reviewer to check findings results and for technical review to verify the accuracy of all SRR checks. They are default* hosts.deny Passwd device.tab inetd.conf PkgInfo devlink.tab Inittab Pslist df-file Last RootCron dgroup.tab localpatches System Group Mnttab VarAdmin Hosts.allow Netstatus Vfstab (NOTE: Directory containing /etc/default files). • guessed.pw.report: A file created in the following directory by running Crack. It is placed in the ~Script/CRACK/SystemName directory. • hostname.Report: A file created by running the Review-Findings program. It summarizes SRR findings in one of five different choices. 15. Run the Manual-Review script. It must be run in this order the first time. Once it has been run for a system, it need not be run again unless the status of a finding changes to Not Reviewed. The Manual-Review script serves these purposes: • Creates system and key personnel information • Creates the Asset record data • Creates the module record data • Allows reviewers to update Not Reviewed items 16. When the Manual-Review program is completed, all items will be filled in (automated and manual). The process includes interviews with the System Administrator/Information System Security Officer, and even the Information Systems Security Manager, for answers to some of the Not Reviewed items. The program will prompt to automatically run the next utility program: SRRDBupdate. Run the Manual-Review from the Script directory with the following command: • ./Manual-Review 17. Run the SRRDBupdate script. It creates the import file for the SRR database and the output name is hostname.txt. The Manual-Review script will automatically execute SRRDBupdate. It prints a dot on the screen for each record it processes. The SRRDBupdate program initially prompts for the name of the system to create the SRR database input file, so it could be used to create outputs for multiple systems as long as the data is provided in a hostname directory under the Script directory. It may be run more than once, as long as the Manual-Review program has been run before it. 18. Execute the script stand-alone, type from the Script directory: • ./SRRDBupdate

Table E-5. SRR Test Procedures: UNIX (continued)

SRR Test Procedures	
Procedures (continued)	19. Run the Review-Findings script. For SRR reviewers, Review-Findings scripts may not be run unless the SRRBDupdate program has been run successfully before. For site users performing self-assessments, it may be run out of order while SRRDBupdate file is tuning the system. For SRR reviewers, it may be run stand-alone at any time after the first time it has been run, and may be run multiple times for different systems. Review-Findings generate the hostname.report with a summary of findings from the SRR. It has five choices for the type of output it produces: • Output all items • Output only open items • Output only Not Reviewed items • Output only Not Applicable items • Output only Not a Finding items 20. The Review-Findings Script must be run after the SRRDBupdate script, which will prompt for execution when it completes. Since the Review-Findings, script produces the output tar file, and the SRRDBupdate script creates the hostname.txt file that must be with it, must be run before it. The Review-Findings script from the Script directory must be run with the following command: • ./Review-Findings 21. Review and validate the findings with the vendor. 22. If time permits, the vendor may remediate any findings that are marked as open. 23. Retrieve the tar file of the SRR data (from the hostname directory) from the system. It is located in the directory above the Script directory by the Review-Findings script. See section E-1.3.1 for instructions on reading the Extensible Markup Language file. 24. Perform a full functionality test.
Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable Data: • VMS Identification Number • Potential Discrepancy Indicator • Number finding that resulted in errors • IA Control information
Collection Form	Information Assurance Assessment Report. DIACAP Scorecard

LEGEND:

DIACAP	DoD Information Assurance Certification and Accreditation Process	HP-UX	Hewlett Packard UNIX
DoD	Department of Defense	PDI	Potential Discrepancy Indicator
IA	Information Assurance	SRR	Security Readiness Review
		SRRDB	Security Readiness Review Data Base

e. Additional IA Requirements. Table E-6 is a cross-matrix of the Generic Requirements (GR)-815 CORE Requirements that are not covered under any current STIG's. These requirements have been included as additional test cases performed during IA testing.

Table E-6. Additional IA Requirements

Test Case	Requirement	Systems Affected	Test Procedure(s)	Risk	Result(s)
1	**Section:** Identification **ID:** R3-6[4] **Reference*:** A **IA Control:** DCSP-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	1. Check to see if the application on the control panel interconnects with numerous distributed applications, switches, routers, or other peripherals. 2. If so, check to see that the login is traceable to each application or device visited. If not, each application, switch, router, or peripheral must require an individual login procedure.	Low	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
2	**Section:** Authentication **ID:** R3-17[42] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	1. At each ingress, attempt to login with an incorrect user-ID. 2. Repeat the login attempt with a correct user-ID but incorrect authenticator. If the login procedure is halted, the SUT fails the test.	Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
3	**Section:** Authentication **ID:** R3-18[43] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	1. At each ingress, attempt to login with an incorrect user-ID. 2. Repeat the login attempt with a correct User-ID, but incorrect authenticator. 3. Check whether the SUT responds with a helpful message (e.g., the User-ID is incorrect, or the password is incorrect). If there is a helpful message, the SUT fails the test.	Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
4	**Section:** Authentication **ID:** R3-25[13] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Login as an administrator and create two user-IDs and assign the same password to both of them. The SUT should allow this transaction. Otherwise it fails the test.	Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
5	**Section:** Authentication **ID:** R3-26[14] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Verify the file storage of passwords (or other authenticator information). If a password is viewable in plaintext, the SUT fails the test.	High	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
6	**Section:** Authentication **ID:** R3-30[18] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Establish a login at each ingress point. Verify that each ingress provides a method for the user to change their password requiring the user to provide a user-ID and an authenticator. If this requirement is not fulfilled, the SUT fails the test.	Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
7	**Section:** System Access Control **ID:** R3-61[236] **Reference*:** A **IA Control:** ECTM-2	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, IAS, and ASLAN	Verify the gateway incorporates screening capabilities.	Medium	

Table E-6. Additional IA Requirements (continued)

Test Case	Requirement	System Affected	Test Procedure(s)	Risk	Result(s)
8	**Section:** System Access Control **ID:** R3-62[237] **Reference*:** A **IA Control:** ECTM-2	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, IAS, and ASVALAN	Ensure IP and TDM SGWs provide screening capabilities.	Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
9	**Section:** System Access Control **ID:** CR3-65[240] **Reference*:** A **IA Control:** DCNR-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	1. Verify that the implementation of SSH2, SSL, IPSEC, AES, SFTP, etc. 2. Verify the cryptographic module is FIPS 140-1 or 140-2 validated. (http://csrc.nist.gov/cryptval/140-1/1401vend.htm) Note: Encryption standards for transporting data may be more stringent dependent upon the deployment strategies.	Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
10	**Section:** System Access Control **ID:** CR3-69[244] **Reference*:** A **IA Control:** DCSR-1	TS, MFS, STP, NMS, EOS, SMEO,DVX, and RSU	Verify message replay detection services.	Low	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
11	**Section:** System Access Control **ID:** CR3-87[55] **Reference*:** A **IA Control:** ECLO-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	At each ingress, establish a successful login and check whether there is a display of the date and time of the last successful login and the number of unsuccessful attempts made since the last login. If not, the SUT fails the test.	Low	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
12	**Section:** Security Audit **ID:** R3-119[83] **Reference*:** A **IA Control:** ECTP-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Initialize the SUT (restart the system) and test whether the history files retain the records. If the records do not survive a system restart, the SUT fails the test.	Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
13	**Section:** Data Integrity **ID:** R3-127[101] **Reference*:** A **IA Control:** DCSQ-1 and ECTM-2	TS, MFS, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Verify that the NE/FS/NS has the capability to protect data integrity by performing integrity checks or data update in the following: 1. Proper rule checking on data update. 2. Adequate alert messages in response to potentially damaging commands before executing them. 3. Proper handling of duplicate or multiple inputs. 4. Checking return status. (Verify unacceptable message return.) 5. Checking intermediate results. (Verify data acceptance.) 6. Checking inputs for reasonable values. (Verify acceptable parameters.)	Low	

Table E-6. Additional IA Requirements (continued)

Test Case	Requirement	System Affected	Test Procedure(s)	Risk	Result(s)
14	**Section:** System Integrity **ID:** R3-129[97] **Reference*:** A	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Verify the NE/FS/NS provides mechanisms to monitor NE/FS/NS resources and their availability (e.g., overflow indication, lost messages, buffer queues).	Low	
	IA Control: ECAT-2				
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
15	**Section:** System Integrity **ID:** R3-130[98] **Reference*:** A **IA Control:** ECAT-2	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Verify the NE/FS/NS provides mechanisms to detect communication errors (relevant to the NE/FS/NS) above a specifiable threshold.	Low	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
16	**Section:** Security Administration **ID:** R3-145[112] **Reference*:** A **IA Control:** ECAR-2	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Verify the capability of the SUT to display all users currently logged in.	Low	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
17	**Section:** Security Administration **ID:** R3-156[123] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Verify the following parameters are not hard-coded: 1. Password Aging Interval, i.e., the length of time the password will remain valid after being updated. Low Risk. 2. The interval (or equivalent) during which an expired user password shall be denied being selected again as a new password by the same user (to prevent “password flipping”). Low Risk. 3. The events that may trigger alarms (e.g., failed login attempts), the levels of alarms (e.g., critical, major, minor), the type of notification (e.g., beep and/or message), and the routing of the alarm (e.g., specific port). Low Risk. 4. The duration of channel lock-out, this occurs when the threshold on the number of incorrect logins is exceeded. Low Risk. 5. An advisory warning banner that is displayed upon valid system entry regarding unauthorized use, and the possible consequences of violating the warning. High Risk. 6. The duration of the time-out interval. Low Risk. 7. The privilege of a user to access a resource. Low Risk. 8. The privilege of a channel/port (for an NE/FS/NS that has different input channels/ports for different operations functions) to access a resource. Low Risk.	Low/Medium	

Table E-6. Additional IA Requirements (continued)

Test Case	Requirement	System Affected	Test Procedure(s)	Risk	Result(s)
17 (continued)	**Section:** Security Administration **ID:** R3-156[123] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	9. Post-collection audit analysis tools for report generation (i.e., the NE/FS/NS shall provide an appropriate administrator the capability to customize exception reports, summary reports, detailed reports, etc., on specific NE/FS/NS data items, users, or communication facilities). Low Risk.	Low/Medium	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
18	**Section:** Security Administration **ID:** CR3-158[125] **Reference*:** A **IA Control: I**AIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Verify that NE/NF/NS notification to users requiring them to change their passwords is not hard-coded.	Low	
Test Case	**Requirement**	**System Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
19	**Section:** Security Administration **ID:** R3-167[134] **Reference*:** A **IA Control:** IAIA-1	TS, MFS, STP, NMS, EOS, SMEO, DVX, RSU, PBX1, PBX2, VTC, CPE, NE, EC, IAS, and ASLAN	Restart to the system and verify that default User-IDs and password, previously modified by an administrator, are not reverted back to vendor-delivered default User-IDs and passwords.	High	

LEGEND:

AES	Advanced Encryption Standard	LSSGR	Local Switching System General Requirement
ASLAN	Assured Services Local Area Network	MFS	Multi-Function Switch
CAC	Common Access Card	NE	Network Element
CPE	Customer Premise Equipment	NMS	Network Management System
DVX	Deployable Voice Exchange	OTGR	Operations Technology Generic Requirements
EC	Echo Canceller	PBX	Private Branch Exchange
EOS	End Office Switch	RSU	Remote Switching unit
FIPS	Federal Information Processing Standards	SMEO	Small End Office
FS/NS	Functional System/Network System	SSH2	Secure Shell 2
GR	Generic Requirement	SSL	Secure Socket Layer
IAS	Integrated Access Switch/Systems	STP	Signal Transfer Point
ID	Identification	SUT	System Under Test
IP	Internet Protocol	SGW	Security Gateway
IPSEC	Internet Protocol Security	TDM	Time Division Multiplexer
IAS	Integrated Access Switch/System	TS	Tandem Switch LECKIT
LECTRL	Local Exchange Carrier Technical Reference Library	VTC	Video Teleconference

NOTE: The Following Reference Applies.
A – Telcordia Technologies Generic Requirements for Network Elements/Network Systems (NE/NS) Security (A Module of OTGR,FR-439;LSSGR, FR-64; and LECTRL, FD-LECKIT) Telcordia Technologies Generic Requirements GR-815-Core, Issue 2, March 2002
B – National Institute for Standards and Technology, Private Branch Exchange Protection Profile
C – National Institute for Standards and Technology, Private Branch Exchange Test Methodology

f. Internet Protocol version 6 (IPv6) Requirements. Table E-7 lists all of the IA IPv6 test requirements per the UCR2008 and its associated test case.

Table E-7. IPv6 Requirements

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
1	**Section:** System Requirements **ID:** 1 The system shall support dual IPv4 and IPv6 stacks as described in RFC 4213. NOTE: The tunnel requirements are only associated with appliances that provide IP routing functions (e.g., routers). The primary intent of these requirements is to (1) require dual stacks on all UC appliances and (2) allow dual stacks and tunneling on routers. **Reference:** UCR 2008 5.3.5.3	Required: SS, NA, EBC, R, LS, – Conditional: EI	1. Conduct an analysis of the system configurations. 2. Verify traffic generated is accepted in IPv4 and IPv6 format. 3. If tunneling is utilized verify that the tunnel is able to transmit IPv6 to IPv4 and also IPv4 to IPv6. 4. Verify that if tunneling is utilized that it is able to process correct decapsulation checks to discard any IPv6 packets with IPv4 compatible addresses in IPv6 header field.	CAT I	
	IA Control: ECSC-1	**Origin:** RFC 4213 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
2	**Section:** System Requirements **ID:** 1.1 If the system supports routing functions, the system shall support the manual tunnel requirements as described in RFC 4213. **Reference:** UCR 2008 5.3.5.3	Conditional: R, LS	1. Verify that the administrator has the ability to manually configure tunnel requirements. 2. Ensure that changes are successful to allow for secure traffic. 3. Verify that IPv6 packets are transported over IPv4 correctly.	CAT I	
	IA Control: ECSC-1	**Origin:** RFC 4213 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
3	**Section:** System Requirements **ID:** 2 The system shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095. **Reference:** UCR 2008 5.3.5.3	Required: SS, NA, EBC, R, LS, EI	1. Verify that all IPv6 addresses are constructed per the IPv6 format in section 3. of RFC 2460. 2. Ensure the IPv6 format of the address is updated according to RFC 5095 which removes the use of the IPv6 "extension header" called Routing Header.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 5095 and Network STIG v7r1			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
4	**Section:** System Requirements **ID:** 3 The system shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464. NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented. **Reference:** UCR 2008 5.3.5.3	Required: SS, EBC, R, LS, EI	1. Verify that the system is able to transmit IPv6 packets over the network. 2. Verify the Address Token in the packet is not the node's 48-bit MAC address per RFC 1972, but is replaced by the Interface Identifier per RFC 2464. EXAMPLE: The Organizationally Unique Identifier of the Ethernet address (the first three octets) becomes the company_id of the EUI-64 (the first three octets). The fourth and fifth octets of the EUI are set to the fixed value FFFE hexadecimal. The last three octets of the Ethernet address become the last three octets of the EUI-64. For example, the Interface Identifier for an Ethernet interface whose built-in address is, in hexadecimal, 34-56-78-9A-BC-DE would be 36-56-78-FF-FE-9A-BC-DE.	CAT III	
	IA Control: ECSC-1	**Origin:** RFC 2464 and Network STIG v7r1			
5	**Section:** MTU **ID:** 4 The system shall support Path Maximum Transmission Unit (MTU) Discovery (RFC 1981). **Reference:** UCR 2008 5.3.5.3.1	Required: EBC, R, LS, EI (Softphone only)	1. Ensure that when the system sends out a large sized IPv6 packet that it has the ability to break up those packets into smaller packets on the network. 2. Verify that if a node receives a packet too big message the node attempts to reduce the size of the original packet sent according to RFC 1981.	CAT I	
	IA Control: ECSC-1	**Origin:** RFC 1981 and Network STIG v7r1			
6	**Section:** MTU **ID:** 5 The system shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095). NOTE: Guidance on MTU requirements and settings can be found in UCR 2008, Section 5.3.3.10.1.2 Layer 2- Data Link Layer. **Reference:** UCR 2008 5.3.5.3.1	Required: SS, NA, EBC, R, LS, EI	1. Verify that the NIC MTU size is set to 1280 bytes. 2. Create packets that are smaller than that of the minimum MTU of 1280 bytes and ensure that a fragment header is appended to the packet it to allow it to meet the minimum MTU size of 1280 bytes.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 5095 and Network STIG v7r1			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
7	**Section:** MTU **ID:** 6 If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, the system shall ignore the request for the smaller MTU and shall include a fragment header in the packet. NOTE: This is to mitigate an attack where the path MTU is adequate, but the Packet Too Big messages are used to make the packet so small it is inefficient. **Reference:** UCR 2008 5.3.5.3.1 **IA Control:** ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 5095	1. Verify that the NIC MTU size is set to 1280 bytes. 2. Create packets that are smaller than that of the minimum MTU of 1280 bytes and ensure that a fragment header is appended to the packet it to allow it to meet the minimum MTU size of 1280 bytes. 3. Ensure that the traffic is passed correctly with the appended header.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
8	**Section:** Flow Label **ID:** 7 The system shall not use the Flow Label field as described in RFC 2460. **Reference:** UCR 2008 5.3.5.3.2 **IA Control:** ECSC-1	Required: SS, NA, EBC, EI **Origin:** RFC 2460 and Network STIG v7r1	1. Create IPv6 packets with the flow label field set in the IPv6 header. 2. Attempt to send the packet to a host or router that does not support the flow label field as described in 2460. 3. Observe the packet as it passes through that host or router and ensure that it ignores the field when receiving the packet.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
9	**Section:** Flow Label **ID:** 7.1 The system shall be capable of setting the Flow Label field to zero when originating a packet. **Reference:** UCR 2008 5.3.5.3.2 **IA Control:** ECSC-1	Required: SS, NA, EBC, EI **Origin:** RFC 2460 and Network STIG v7r1	1. Attempt to create IPv6 packets with the flow label field set in the IPv6 header. 2. Attempt to send out the IPv6 packet on the network. 2. Ensure that the flow label field on the packet is set to zero.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
10	**Section:** Flow Label **ID:** 7.2 The system shall not modify the Flow Label field when forwarding packets. **Reference:** UCR 2008 5.3.5.3.2 **IA Control:** ECSC-1	Required: SS, NA, EBC **Origin:** RFC 2460 and Network STIG v7r1	1. Create IPv6 packets with the flow label field set in the IPv6 header. 2. Attempt to send out the IPv6 packet through the system tested host or router. 3. Ensure that the Flow Label field set in the header of the IPv6 packets created when passed through the host or router on the network are not modified.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
11	**Section:** Flow Label **ID:** 7.3 The system shall be capable of ignoring the Flow Label field when receiving packets. **Reference:** UCR 2008 5.3.5.3.2	Required: SS, NA, EBC, EI	1. Create IPv6 packets with the flow label field set in the IPv6 header. 2. Send out the IPv6 packet on to the system under test. 3. Ensure that the Flow Label field is ignored and that the system does not process the packet according to the Flow Label Field in the IPv6 header.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2460 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
12	**Section:** Address **ID:** 8 The system shall support the IPv6 Addressing Architecture as described in RFC 4291. NOTE: The use of "IPv4 Mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities. **Reference:** UCR 2008 5.3.5.3.3	Required: SS, NA, EBC, R, LS, EI	1. Verify the system is capable of communication through IPv6. 2. Ensure that the system follows the IPv6 Addressing Architecture in RFC 4291. 3. Ensure that the system does not use IPV4 mapped IPv6 addresses due to improper handling by some IPv4 devices.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4291 and Network STIG v7r1			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
13	**Section:** DHCP **ID:** 10 If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 system, it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315. NOTE 1: UCR 2008, Section 5.4, Information Assurance, requires that the voice or video DHCP servers are not to be located on the same physical appliance as the voice or video LAN switches and routers in accordance with the Security Technical Implementation Guides (STIGs). Also, the VoIP STIG requires (in VoIP 0082) separate DHCP servers for (1) the phone system in the phone VLAN(s) and (2) the data devices (PCs) in the data VLAN(s). NOTE 2: There is no requirement that separate DHCP servers be used for IPv4 and for IPv6. **Reference:** UCR 2008 5.3.5.3.4	Conditional: SS, NA EI, R, LS	1. Confirm that the system is capable of utilizing DHCP Note: If the system does not use DHCP services, this requirement test procedure is not applicable. 2. Determine the Identify of the DHCP server. 3. Configure the system to obtain an IP address through dynamic allocation as opposed to automatic or manual allocation. 1. Ensure the system attempts to connect to the DHCP server and that the traffic passed between the systems and the IP addressing is processed securely. 2. Perform functionality checks to verify that it is capable of communication with the new address.	CAT II	
	IA Control: DCCS-2 and DCPA-1	**Origin:** RFC 3315			
14	**Section:** DHCP **ID:** 10.1 If the system is a DHCPv6 client, the system shall discard any messages that contain options that are not allowed, which are specified in Section 15 of RFC 3315. **Reference:** UCR 2008 5.3.5.3.4	Conditional: SS, NA, EI	1. Verify that DHCP is currently in use. 2. Attempt to send a DHCP message to the client with an improper option set for the message. (e.g., an Identity Association option in an Information-Request message). 3. Observe the actions of the host to ensure that the message is discarded.	CAT II	
	IA Control: DCBP-1 ECSC-1	**Origin:** RFC 3315			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
15	**Section:** DHCP **ID:** 10.2 The system shall support DHCPv6 as described in RFC 3315. NOTE: The following subtended requirements are predicated upon an implementation of DHCPv6 for the end instrument. It is not expected that other UC appliances will use DHCPv6. **Reference:** UCR 2008 5.3.5.3.4	Required: EI	1. Confirm that the system is capable of utilizing DHCP Note: If the system does not use DHCP services, this requirement test procedure is not applicable. 2. Configure the system to obtain an IP address through dynamic allocation as opposed to automatic or manual allocation. 3. Verify that the system supports the ability of obtaining a new IP address from the DHCP server. 4. Observe the traffic between the host and the DHCP server to insure that it is correctly processing the DHCP requests per RFC 3315.	CAT II	
	IA Control: DCSP-1 and ECSC-1	**Origin:** RFC 3315			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
16	**Section:** DHCP **ID:** 10.2.1 If the system is a DHCPv6 client, and the first Retransmission Timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, the client shall continue with a client-initiated message exchange by sending a Request message. **Reference:** UCR 2008 5.3.5.3.4	Required: EI Conditional: SS, NA	1. Verify that DHCP is currently in use. 2. Send a solicit message from the system under test. 3. Ensure that an Advertise message with a preference value of 255 is sent to the host. 4. Once the host receives the advertise message observe traffic between the host and the DHCP server 5. Verify that the client initiates a request message.	CAT II	
	IA Control: DCBP-1 and ECSC-1	**Origin:** RFC 3315			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
17	**Section:** DHCP **ID:** 10.2.2 If the system is a DHCPv6 client and the DHCPv6 message exchange fails, it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs. NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds. **Reference:** UCR 2008 5.3.5.3.4 **IA Control:** DCBP-1 and ECSC-1	Required: EI Conditional: SS, NA **Origin:** RFC 3315	1. With the system under test attempt to initiate a message exchange to a DHCPv6 server 2. Ensure that the message exchange between the system under test and the DHCP server fails. 3. After the failure of the message exchange fails attempt to restart the process through user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event. 4. Verify that the reconfiguration process restarts and the client attempts to communicate with the server.	CAT II	
18	**Section:** DHCP **ID:** 10.2.3 If the system is a DHCPv6 client and it sends an Information-Request message, it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server. **Reference:** UCR 2008 5.3.5.3.4 **IA Control**: ECSC-1	Required: EI Conditional: SS, NA **Origin:** RFC 3315	1. With the system being tested initiate an information request message to the DHCPv6 server 2. Attempt to send an information request without a Client Identifier and ensure that the system is unable to be authenticated to the DHCPv6 server 3. Attempt to send an information request with a Client Identifier and ensure that the system is now able to be authenticated to the DHCPv6 server.	CAT II	
19	**Section:** DHCP **ID:** 10.2.4 If the system is a DHCPv6 client, it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server prior to transmitting packets using that address for itself. **Reference:** UCR 2008 5.3.5.3.4 **IA Control:** ECSC-1	Required: EI Conditional: SS, NA **Origin:** RFC 3315	1. Prepare the system under test to request an address from the DHCPv6 server. 2. Ensure that the server attempts to assign the system an address that is already in use by another client. 3. Observe the actions of the system to ensure that it sends a decline message back to the DHCP server to inform it that the address assigned is already in use.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
20	**Section:** DHCP **ID:** 10.2.5 If the system is a DHCPv6 client, it shall log all reconfigure events. **Reference:** UCR 2008 5.3.5.3.4 **IA Control**: ECSC-1	Required: EI Conditional: SS, NA **Origin:** RFC 3315	1. Complete a configuration change to the DHCP server to ensure that it will send out a reconfigure message to the system under test. 2. Ensure that once the client receives the reconfigure message that the message is logged. 3. Confirm the logging of the reconfigure message by the client.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
21	**Section:** DHCP **ID:** 10.3 If the system supports DHCPv6 and uses authentication, it shall discard unauthenticated DHCPv6 messages from UC systems and log the event. NOTE: This requirement assumes authentication is used as described in RFC 3118 (and extended in RFC 3315) but does not require authentication. **Reference:** UCR 2008 5.3.5.3.4 **IA Control:** DCBP-1 and ECSC-1	Conditional: SS, NA, EI, R, LS **Origin:** RFC 3315	1. Send out an Advertise message from the DHCP server without authentication information included. 2. Ensure that the system under test receives the message and discards the message due to it being unauthenticated. 3. Confirm the logging of the unauthenticated advertise message by the client.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
22	**Section:** Neighbor Discovery **ID:** 11 The system shall support Neighbor Discovery for IPv6 as described in RFC 2461 and RFC 4861 (FY2010). **Reference:** UCR 2008 5.3.5.3.5 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4861	1. Connect the system under test to a properly configured test network. 2. Once the system is connected to the network view traffic from the host to ensure that it properly attempts to use the proper protocols for Neighbor Discovery defined in RFC 2461. (e.g. *Router Discovery* to locate routers on their local network, *Parameter Discovery* to determine link parameters such as the link MTU, also *Duplicate Address Detection* to determine that an address the host wishes to use is not already in use.)	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
23	**Section:** Neighbor Discovery **ID:** 11.1 The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. **Reference:** UCR 2008 5.3.5.3.5	Required: SS, NA, EBC, R, LS	1. Attempt to send a neighbor advertisement message from the host. (e.g. *Neighbor Solicitation*: Sent by a node to determine the link-layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link-layer address. Neighbor Solicitations are also used for Duplicate Address Detection. *Anycast addresses:* Anycast addresses identify one of a set of nodes providing an equivalent service, and multiple nodes on the same link may be configured to recognize the same anycast address. Neighbor Discovery handles anycasts by having nodes expect to receive multiple Neighbor Advertisements for the same target. All advertisements for anycast addresses are tagged as being non-Override advertisements. A non-Override advertisement is one that does not update or replace the information sent by another advertisement. *Proxy advertisements*: A node willing to accept packets on behalf of a target address that is unable to respond to Neighbor Solicitations can issue non-Override Neighbor Advertisements. Proxy advertisements are used by Mobile IPv6 Home Agents to defend mobile nodes' addresses when they move off-link. However, it is not intended as a general mechanism to handle nodes that, e.g., do not implement this protocol.) 2. Ensure that the override flag bit is not set in the advertisement message which in turn does not overwrite previous information identified in past messages.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
24	**Section:** Neighbor Discovery **ID:** 11.2 The system shall set the override flag bit in the neighbor advertisement message to “1” if the message is not an anycast address or a unicast address for which the system is providing proxy service. **Reference:** UCR 2008 5.3.5.3.5	Required: SS, NA, EBC, R, LS	1. Attempt to send a Neighbor Advertisement message by the host to a specified target system that sends a Neighbor Solicitation message to start the communication process. 2. In response to the Neighbor Solicitation message the system under test will set the override flag bit to “1” in the Neighbor Advertisement message sent back to the target address. (Proper setting of the Override flag ensures that nodes give preference to non-proxy advertisements, even when received after proxy advertisements, and also ensures that the first advertisement for an anycast address "wins".)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
25	**Section:** Neighbor Discovery **ID:** 11.3 If a valid neighbor advertisement is received by the system and the system neighbor cache does not contain the target’s entry, the advertisement shall be silently discarded. **Reference:** UCR 2008 5.3.5.3.5	Conditional: SS, NA, EBC, R, LS, EI	1. Attempt to send a Neighbor Advertisement message to the system under test with a preconfigured test client on the network in which the system under test will not have the address for the client in its neighbor cache which is used to inform the system of neighbors on the network in which traffic has been initiated with. 2. Verify that when the system under test receives the neighbor advertisement from the client the advertisement is discarded.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
26	**Section:** Neighbor Discovery **ID:** 11.4 If a valid neighbor advertisement is received by the system and the system neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the system shall silently discard the received advertisement. **Reference:** UCR 2008 5.3.5.3.5	Conditional: SS, NA, EBC, R, LS, EI	1. Attempt to send a Neighbor Advertisement message to the system under test when its neighbor cache is an INCOMPLETE state. (i.e. INCOMPLETE: Address resolution is in progress and the link-layer address of the neighbor has not yet been determined.) 2. Verify that when the system under test receives the neighbor advertisement while in INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included that the message is discarded.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
27	**Section:** Neighbor Discovery **ID:** 11.5 If address resolution fails on a neighboring address, the entry shall be deleted from the system's neighbor cache. **Reference:** UCR 2008 5.3.5.3.5	Conditional: SS, NA, EBC, R, LS, EI	1. Initiate address resolution for a neighboring address on the network. 2. Ensure that the system under test creates an entry in the INCOMPLETE state and initiates the address resolution process. 3. Verify that the address resolution process fails and that the entry for the client is deleted from the system's neighbor cache. (i.e. The entry is deleted so that subsequent traffic to that neighbor invokes the next-hop determination procedure once again to allow for the system to attempt to find an alternate route to communicate with the host.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
28	**Section:** Redirect Messages **ID:** 11.6 The system shall support the ability to configure the system to ignore redirect messages. **Reference:** UCR 2008 5.3.5.3.5.1	Required: SS, NA, EBC, EI	1. Configure the system under test to ignore redirect message. 2. Generate a redirect message from a router on the test network to inform the system under test of an alternate route to take for traffic. 3. Verify that the system receives the redirect message from the router and that the system ignores the message.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4890			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
29	**Section:** Redirect Messages **ID:** 11.7 The system shall only accept redirect messages from the same router as is currently being used for that destination. NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a redirect message from router X for packets destined for location A to be sent to router Z. **Reference:** UCR 2008 5.3.5.3.5.1	Required: SS, NA, EBC, R, LS, EI	1. Attempt to send a packet from the system under test to a pre-determined router configured on the test network. 2. Then attempt to send a redirect message to the system from a different router on the test network in which the original packet generated must travel through to reach its destination. 3. Verify that the system receives the redirect message from the router and that the system ignores the message.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2461			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
30	**Section:** Redirect Messages **ID:** 11.7.1 If redirect messages are allowed, the system shall update its destination cache in accordance with the validated redirect message. **Reference:** UCR 2008 5.3.5.3.5.1	Conditional: SS, NA, EBC, R, LS, EI	1. Attempt to send a packet from the system under test to a pre-determined router configured on the test network. 2. Attempt to send a redirect message from the router on the test network in which the system is using to relay its packet to the destination. 3. Verify that the system receives the validated redirect message (per Section 8.1 RFC 4861) from the router and that the system updates its destination cache for future traffic.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2461			
31	**Section:** Redirect Messages **ID:** 11.7.2 If the valid redirect message is allowed and no entry exists in the destination cache, the system shall create an entry. **Reference:** UCR 2008 5.3.5.3.5.1	Conditional: SS, NA, EBC, R, LS, EI	1. Send the system under test a valid redirect message from a router set to process traffic for the host in which the redirect message contains a new address for which the system is unaware of. 2. Verify that when the system receives the redirect message that it updates its destination cache to include the new address contained in the redirect message.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2461			
32	**Section:** Router Advertisements **ID:** 11.8 If the system sends router advertisements, the system shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements. **Reference:** UCR 2008 5.3.5.3.5.2	Required: R Conditional: LS, EBC	1. Configure a router on the test network to send out an inconsistent router advertisement to the system under test. (i.e. Information to determine what makes a router advertisement a valid advertisement can be found in section 6.2.7. Router Advertisement Consistency of RFC 4861.) 2. Ensure that when the system receives the router advertisement it attempts to validate it and when it fails that the inconsistent router advertisement is logged.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
33	**Section:** Router Advertisements **ID:** 11.8.1 The system shall prefer routers that are reachable over routers whose reachability is suspect or unknown. **Reference:** UCR 2008 5.3.5.3.5.2	Required: SS, NA, EBC, EI	1. Configure the system under test to send out packets through neighboring routers. 2. On the closest router to the system for the test ensure that the connection is unreliable for the system under test. 3. On the next router on the network verify that it has a good connection to send traffic on. 4. Send out a packet to a destination on the network and verify the system attempts to reference a previous reachability confirmation to send the packet through the router that it knows is accessible and that it does not attempt to first send the packet through the router on the network configured with an unreliable connection.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
34	**Section:** Router Advertisements **ID:** 11.9 If the system sends router advertisements, the system shall include the MTU value in the router advertisement message for all links in accordance with RFC 2461 and RFC 4861 (FY2010). **Reference:** UCR 2008 5.3.5.3.5.2	Required: R Conditional: LS, EBC	1. Attempt to send a router advertisement message with the system under test. 2. Verify that the router advertisement message contains the MTU value for that link. (i.e. MTU values should be included in router advertisements to verify that they are in fact valid advertisements. Information used to determine that a router advertisement is in fact valid can be found in section 6.2.7 Router Advertisement Consistency in RFC 4861.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4861			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
35	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12 If the system supports stateless IP address autoconfiguration, the system shall support IPv6 Stateless Address Auto-Configuration (SLAAC) for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862 (FY2010). **Reference:** UCR 2008 5.3.5.3.6	Required: R, LS, EI (Softphone only) Conditional: SS, NA, EBC, EI	1. Connect the system under test to the test network without an address specified for the specific interface. 2. Once connected to the network verify that the system begins the auto-configuration process by generating a link-local address for the interface. 3. The system will then attempt to send out a Neighbor Solicitation message to ensure that the address for the interface is not already in use on the network. 4. Next ensure the system attempts to receive a router advertisement message to determine what routers if any are available on the network.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4862			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
36	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.1 The system shall have a configurable parameter that allows the “managed address configuration” flag and the “other stateful configuration” flag to always be set and not perform stateless autoconfiguration. NOTE: The objective of this requirement is to prevent a system from using stateless auto configuration. **Reference:** UCR 2008 5.3.5.3.6	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system is configurable to have the “managed address configuration” flag and the “other stateful configuration” flag to always be set (i.e. A "managed address configuration" flag indicates whether hosts should use stateful autoconfiguration to obtain addresses. An "other stateful configuration" flag indicates whether hosts should use stateful autoconfiguration to obtain additional information (excluding addresses.) 2. Configure the flags to be set to prevent stateless auto-configuration. 3. Connect the system to the network and verify that it does not attempt to start the stateless auto-configuration process as defined in Section 4 of RFC 2462.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
37	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.2 The system shall support manual assignment of IPv6 addresses. **Reference:** UCR 2008 5.3.5.3.6	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system under test is capable of being configured to allow for the manual input of an IPv6 address. 2. Assign an address to the system that will allow for it to communicate on a test network. 3. Connect the system to the network and verify connectivity of the system.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
38	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.3 The system shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE). NOTE: This requirement is associated with the earlier requirement for the EI to support DHCPv6. **Reference:** UCR 2008 5.3.5.3.6	Required: EI	1. Configure the system under test to have the ManagedFlag value set to TRUE. (The Default setting for the ManagedFlag value on a system is set to FALSE.) 2. Connect the system to the network and verify that it does not attempts to start the stateless auto-configuration process, as stateful auto-configuration is used to assign an address manually to the system	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
39	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.3.1 If the system sends router advertisements, the system shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful autoconfiguration is implemented. **Reference:** UCR 2008 5.3.5.3.6	Required: R Conditional: LS, EBC	1. Verify that the system under test is configurable to allow for the "managed address configuration" flag and the "other stateful flag" to be set to TRUE 2. Attempt to send out a router advertisement from the system under test to a target host on the network. 3. Verify that the router advertisement contains the "managed address configuration" flag and the "other stateful flag" set to TRUE. (i.e. In addition, when the value of the ManagedFlag is TRUE, the value of OtherConfigFlag is implicitly TRUE as well. It is not a valid configuration for a host to use stateful address autoconfiguration to request addresses only, without also accepting other configuration information.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			
40	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.4 If the system supports a subtended appliance behind it, the system shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the system and does not cause the system to attempt to change its IP address. NOTE: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address. **Reference:** UCR 2008 5.3.5.3.6	Conditional: EI	1. Configure a phone system on the test network with a hub or switch interface in which the system may connect to the network through. 2. Connect the system to the switch interface of the phone system on the test network. 3. Verify the system is able to obtain an IP address on the network to allow for connectivity. 4. Once the system has obtained its IP address and it is capable of communicating on the network ensure that the configuration of the phone system is unchanged and that it retained it's original IP address.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3756			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
41	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.5 If the system supports IPv6 SLAAC, the system shall have a configurable parameter that allows the function to be enabled and disabled. **Reference:** UCR 2008 5.3.5.3.6	Conditional: SS, NA, EBC, EI	1. Verify that the system under test is configurable to allow for the SLAAC to be enabled or disabled. (e.g. Per RFC 2462 Hosts maintain the following variables on a per-interface basis: ManagedFlag: Copied from the M flag field (i.e., the "managed address configuration" flag) of the most recently received Router Advertisement message. The flag indicates whether or not addresses are to be configured using the stateful autoconfiguration mechanism. It starts out in a FALSE state. OtherConfigFlag: Copied from the O flag field (i.e., the "other stateful configuration" flag) of the most recently received Router Advertisement message. The flag indicates whether or not information other than addresses is to be obtained using the stateful autoconfiguration mechanism. It starts out in a FALSE state. In addition, when the value of the ManagedFlag is TRUE, the value of OtherConfigFlag is implicitly TRUE as well. It is not a valid configuration for a host to use stateful address autoconfiguration to request addresses only, without also accepting other configuration information.) 2. Enable SLAAC on the system and connect it to the network and ensure that it begins the stateless auto-configuration process. 3. Disable SLAAC on the system and connect it to the network and ensure that it does not begin the stateless auto-configuration process.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
42	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.6 If the system supports SLAAC and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPsec capable systems shall support privacy extensions for stateless address autoconfiguration as defined in RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6. **Reference:** UCR 2008 5.3.5.3.6	Conditional: EI (Softphones only)	1. Configure the system under test to allow the use of IPsec and to . 2. Connect the system to the test network and verify that it attempts to create a new randomized interface identifier. (i.e. A new interface identifier can be created by a few different methods which are explained in Section 3 of RFC 4941.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4941			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
43	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.7 If the system supports stateless IP address autoconfiguration, the system shall support a configurable parameter to enable or disable manual configuration of the site-local and Global addresses (i.e., disable the “Creation of Global and Site-Local Addresses” as described in Section 5.5 of RFC 2462). **Reference:** UCR 2008 5.3.5.3.6	Required: R, LS, EI (Softphone only) Conditional: SS, NA, EBC, EI	1. Verify that the system under test is configurable for the enabling and or disabling of manual configuration of site-local and Global addresses. 2. Configure the system under test with a site-local address and attempt to have a host in a separate network reach the system in the test network 3. Verify that the system with the site-local address is unreachable from the host on a separate network. 4. Configure the system under test with a Global routing prefix and attempt to have a host in a separate network reach the system in the test network 5. Verify that the system with the Global routing prefix is reachable by the host on a separate network.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
44	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.8 All IPv6 nodes shall support link-local address configuration, and the Duplicate Address Detection (DAD) shall not be disabled in accordance with RFC 2462 and RFC 4862 (FY2010). **Reference:** UCR 2008 5.3.5.3.6 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4862	1. Attempt to connect the system under test to the test network. 2. Verify that the system attempts to assign a link-local address to its interface. 3. Once the system attempts to assign a link-local address verify that it attempts to perform Duplicate Address Detection to ensure that it is not using an address that is already assigned to a separate host on the network.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
45	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14 The system shall support the Internet Control Message Protocol for IPv6 (ICMPv6) as described in RFC 4443. **Reference:** UCR 2008 5.3.5.3.7 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4443	1. Conduct an analysis of the system configuration. 2. Verify that ICMPv6 is implemented as the IPv6 messaging protocol. 3. Ensure that the protocol is configured properly per Section 2 of RFC 4443.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
46	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.1 The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. **Reference:** UCR 2008 5.3.5.3.7 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4443	1. Confirm that the system is capable of configuring rate limiting. 2. Verify that you have the ability to set the parameter for rate limiting to a desired rate. 3. After you have configured rate limiting to a determined rate generate ICMP traffic that would surpass the rate limiting parameter you previously configured and ensure that the traffic is either dropped or delayed on that interface.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
47	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.2 The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. **Reference:** UCR 2008 5.3.5.3.7 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS **Origin:** RFC 4443	1. Confirm that ICMPv6 is in use on the system under test. 2. Certify that the system has the ability to enable and disable Destination Unreachable Messages. 3. Configure a host on the test network to not allow ICMP traffic through a firewall. 4. Verify that the system has the ability to generate the Destination Unreachable message. 5. Send an ICMP packet to the system setup to not allow ICMP traffic and ensure that a Destination Unreachable message is returned.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
48	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.3 The system shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast/anycast address. NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack. **Reference:** UCR 2008 5.3.5.3.7	Required: SS, NA, EBC, R, LS, EI	1. Confirm that ICMPv6 is in use on the system under test. 2. Certify that the system has the ability to enable and disable Echo Reply Messages. 3. Verify that the system tested first has Echo Reply disabled then send an Echo Request from a host on the test network and ensure that no Echo Reply is received. 4. Verify that the system tested has Echo Reply enabled then send an Echo Request from a host on the test network and ensure that an Echo Reply is received.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4443			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
49	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.4 The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them. **Reference:** UCR 2008 5.3.5.3.7	Required: SS, NA, EBC, R, LS, EI	1. Configure an ICMP message with information contained in the payload of the message. 2. As the ICMP message is sent from the host intercept the message from another system on the test network and attempt to perform a change to the information contained in the payload of the ICMP message. 3. Verify that the system tested attempts to validate the ICMP before acting on the information contained in the payload.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4443			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
50	**Section:** Routing Functions **ID:** 15 If the system supports routing functions, the system shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 2740. **Reference:** UCR 2008 5.3.5.3.8	Required: R Conditional: LS	1. Conduct an analysis of the system configuration and verify the router configuration. 2. Verify that routing functions are configured to support the OSPF for IPv6 methodologies.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2740			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
51	**Section:** Routing Functions **ID:** 15.1 If the system supports routing functions, the system shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.8	Required: R Conditional: LS	1. Verify that routing functions are configured to support the OSPF for IPv6 methodologies. 2. Analyze network traffic to determine if IPSec is used to secure the routing functions.	CAT II	
	IA Control: ECSC-1	**Origin:** UCR 2008, Section 5.4, Information Assurance			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
52	**Section:** Routing Functions **ID:** 15.2 If the system supports routing functions, the system shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-128 as described in RFC 4302. **Reference:** UCR 2008 5.3.5.3.8	Required: R Conditional: LS	1. Examine the system configuration and verify that routing functions are supported. 2. Ensure that router-to-router communications are secured by using the IP Authentication Header with HMAC-SHA1-128 encryption.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4302			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
53	**Section:** Routing Functions **ID:** 16 If the system acts as a CE router, the system shall support the use of Border Gateway Protocol (BGP) as described in RFC 1772 and 4271 **Reference:** UCR 2008 5.3.5.3.8	Conditional: R	1. Inspect the system under test to verify its use as a Customer Edge Router. 2. Ensure that another router setup on a test network is able to communicate to the system under test. 3. Generate traffic on the test network where the system under test would need to update its routing tables. 4. Ensure that when the router on a separate test network attempts to communicate with the system under test that it is able to exchange its routing information per RFC 4271.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4271			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
54	**Section:** Routing Functions **ID:** 16.1 If the system acts as a customer edge router, the system shall support the use of BGP-4 multiprotocol extensions for IPv6 Inter-Domain routing (RFC 2545). NOTE: The requirement to support BGP-4 is in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements. **Reference:** UCR 2008 5.3.5.3.8	Conditional: R	1. Configure the test network for IPv6 communication. 2. Ensure that the system under test supports BGP-4 per RFC 2545 and allows for Inter Domain Routing for IPv6. (i.e. In terms of routing information, the most significant difference between IPv6 and IPv4 (for which BGP was originally designed) is the fact that IPv6 introduces scoped unicast addresses and defines particular situations when a particular address scope must be used.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2545			
55	**Section:** Routing Functions **ID:** 17 If the system acts as a CE router, the system shall support multiprotocol extensions for BGP-4 RFC 2858 and RFC 4760 (FY2010). NOTE: The requirement to support BGP-4 is in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements. **Reference:** UCR 2008 5.3.5.3.8	Conditional: R, LS	1. Verify that the CE router allows for support of BGP-4. 2. Document the use of the NEXT_HOP attribute and also the use of Network Layer Reachability Information for its support of IPv4 and IPv6.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4760			
56	**Section:** Routing Functions **ID:** 18 If the system acts as a CE router, the system shall support the Generic Routing Encapsulation (GRE) as described in RFC 2784. **Reference:** UCR 2008 5.3.5.3.8	Conditional: R	1. The system under test should allow for the support of Generic Routing Encapsulation per RFC 2784. 2. Ensure that you have the ability to create a tunnel between the system under test and another router configured. 3. Make sure that the traffic between the two routers is being encapsulated and that the routers are able to properly communicate.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2784			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
57	**Section:** Routing Functions **ID:** 19 If the system acts as a CE router, the system shall support the Generic Packet Tunneling in IPv6 Specification as described in RFC 2473. NOTE: Tunneling is provided for data applications and is not needed as part of the VVoIP architecture. **Reference:** UCR 2008 5.3.5.3.8 **IA Control:** ECSC-1	Conditional: R **Origin:** RFC 2473	1. The system shall allow the ability for the tunneling between two nodes on the network. 2. Attempt to create a tunnel between two nodes to communicate on the network. 3. Once the tunnel has been established verify that the two nodes do not have any issues with communication. 4. Analyze the network traffic and verify that it is being encapsulated and decapsulated by the nodes on the tunnel.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
58	**Section:** Routing Functions **ID:** 20 If the system supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. NOTE: The FY 2008 VVoIP design does not utilize multicast, but routers supporting VVoIP also support data applications that may utilize multicast. A softphone will have non-routing functions that require MLDv2. **Reference:** UCR 2008 5.3.5.3.8 **IA Control**: ECSC-1	Required: R, EI(Softphone) Conditional: LS **Origin:** RFC 3810	1. Conduct an analysis of the systems configuration and verify that it supports Multicast Listener Discovery. 2. Make certain that the system under test has the ability to discover multicast listeners on directly attached links. 3. Verify that the system has the ability to discover multicast addresses which are of interest to neighboring nodes. 4. If MLDv2 is supported MLDv2 provides for source filtering to allow nodes to listening to packets only from specific sources.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
59	**Section:** Routing Functions **ID:** 21 The system shall support MLD as described in RFC 2710. NOTE: This requirement was added in order to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement. **Reference:** UCR 2008 5.3.5.3.8 **IA Control:** ECSC-1	Required: SS, NA, EBC, EI, LS **Origin:** RFC 2710	1. Conduct an analysis of the systems configuration and verify that it supports Multicast Listener Discovery. 2. Make certain that the system under test has the ability to discover multicast listeners on directly attached links. 3. Verify that the system has the ability to discover multicast addresses which are of interest to neighboring nodes.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
60	**Section:** IP Security **ID:** 22 If the system uses IPSec, the system shall support the Security Architecture for the IP RFC 2401 and RFC 4301 (FY2010). In FY2008, RFC 2401 (and its related RFCs) is the Threshold requirement as described in UCR 2008, Section 5.4, Information Assurance. In addition, the interfaces required to use IPSec are defined in UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify that the system supports the use of IPSec. 2. Ensure that the system has the ability to communicate with another host on the network with IPSec in use. 3. Analyze the network traffic to ensure communication between the hosts is encrypted and that both hosts are communicating properly according to RFC 2401 and RFC 4301.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
61	**Section:** IP Security **ID:** 22.1 If RFC 4301 is supported, the system shall support binding of a security association (SA) with a particular context. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Certify that IPSec is currently in use by the system. 2. Configure the system under test to allow for the ability to bind separate security associations on the test network to a particular context. (e.g. A security gateway that provides VPN service to multiple customers will be able to associate each customer's traffic with the correct VPN.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
62	**Section:** IP Security **ID:** 22.2 If RFC 4301 is supported, the system shall be capable of disabling the BYPASS IPSec processing choice. NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify that IPSec is in use by the system. 2. Ensure that the system does not have the ability to enable the BYPASS IPSec option for the Security Policy Database. 3. Attempt to set the process choice of BYPASS IPSec in the Security Policy Database and verify that you are unable to do so.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
63	**Section:** IP Security **ID:** 22.3 If RFC 4301 is supported, the system shall not support the mixing of IPv4 and IPv6 in a security association. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4301	1. Create a security association between the system under test and a separate host. 2. Attempt to communicate in the Security Association with IPv6 traffic and verify that a connection is made correctly. Also attempt to communicate with IPv4 traffic and verify that a connection is made correctly. 3. Verify that the security association does not provide the ability to use both IPv4 and IPv6 traffic on a single security association.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
64	**Section:** IP Security **ID:** 22.4 If RFC 4301 is supported, the system's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. NOTE: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, describes a scenario where this could occur. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4301	1. Ensure that the Security Association Database has the ability to create a separate entry for each host in a specific security association. 2. Verify the systems ability to create a unique entry for each host in a security association. (i.e. This may be done through a unique identifier for each system on the network) (Section 4.4.2 per RFC 4301 explains the situation where a SAD entry could be associated with multiple SA's: For instance, two hosts behind the same NAT could choose the same SPI value. The situation also may arise if a host is assigned an IP address (e.g., via DHCP) previously used by some other host, and the SAs associated with the old host have not yet been deleted via dead peer detection mechanisms. This may lead to packets being sent over the wrong SA or, if key management ensures the pair is unique, denying the creation of otherwise valid SAs. Thus, implementors should implement links between the SPD cache and the SAD in a way that does not engender such problems.)	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
65	**Section:** IP Security **ID:** 22.5 If RFC 4301 is supported, the system shall be capable of correlating the Differentiated Services Code Point (DSCP) for a VVoIP stream to the security association in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements and Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan. For a more detailed description of the requirement, please see Section 4-1 of RFC 4301 - Security Architecture for the Internet Protocol. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Prepare the system under test to process traffic for a number of different security associations that are configured. 2. Verify that the system has the ability to properly correlate the DSCP values on packets and route those packets to the appropriate security association mapped to that DSCP value of the traffic.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
66	**Section:** IP Security **ID:** 22.6 If RFC 4301 is supported, the system shall implement IPSec to operate with both integrity and confidentiality. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify the system has the ability to operate IPSec with integrity and confidentiality. 2. Integrity and Confidentiality in IPSec is completed through the use of the IP Authentication Header and the Encapsulating Security Payload.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
67	**Section:** IP Security **ID:** 22.7 If RFC 4301 is supported, the system shall be capable of enabling and disabling the ability of the system to send an ICMP message informing the sender that an outbound packet was discarded. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Confirm that ICMPv6 is in use on the system under test. 2. Certify that the system has the ability to enable and disable ICMP error messages such as that of an ICMP PMTU error message. 3. Send an ICMP packet outbound that will be discarded; For example sending a packet larger than that of a security associations PMTU in which fragmentation is not enabled. 4. Verify that if the ability to send an ICMP error message is enabled the system sends out an ICMP error message, also verify that if the ability to send an ICMP error message is disabled the system does not send out an ICMP error message.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
68	**Section:** IP Security **ID:** 22.7.1 If an ICMP outbound packet message is allowed, the system shall be capable of rate limiting the transmission of ICMP responses **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Confirm that the system is capable of configuring rate limiting. 2. Verify that you have the ability to set the parameter for rate limiting to a desired rate. 3. After you have configured rate limiting to a determined rate Attempt to spoof a system on the network with a source address already in use, then send out packets to another system on the network to elicit it to send ICMP packets to the original system in which you spoofed its source address. 4. Ensure that with rate limiting set that the system in which you spoofed on the network only receives a limited amount of ICMP packets before they are discarded or delayed.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
69	**Section:** IP Security **ID:** 22.8 If RFC 4301 is supported, the system shall be capable of enabling or disabling the propagation of the Explicit Congestion Notification (ECN) bits. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Ensure that the system has the ability to enable and disable Explicit Congestion Notification bits. 2. Next Generate a large amount of traffic on the network in which without Explicit Congestion Notification enabled the packets directed at a particular host would be discarded due to the high volume of traffic. 3. Now with Explicit Congestion Notification enabled attempt to create that large amount of traffic to communicate with a specific host, verify that the packets are not discarded, but are labeled with the Explicit Congestion Notification bits to allow the continuous communication between the sources.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
70	**Section:** IP Security **ID:** 22.9 If RFC 4301 is supported, the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. View the Security Policy Database for the IPSec Implementation. 2. Ensure that the final entry in the Security Policy Database is set to discard any traffic that is not already identified as being mapped to the Security Policy Database to specify secure communications.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
71	**Section:** IP Security **ID:** 22.10 If RFC 4301 is supported, and the system receives a packet that does not match any SPD cache entries and the system determines it should be discarded, the system shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Attempt to communicate through a security association with a separate host by means of which you have set to not allow in the Security Policy Database. 2. Verify that the packet is discarded and that the system logs the event and includes the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
72	**Section:** IP Security **ID:** 22.11 If RFC 4301 is supported, the system should include a management control to allow an administrator to enable or disable the ability of the system to send an Internet Key Exchange (IKE) notification of an INVALID_SELECTORS. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify that the system is capable of enabling and disabling the sending of an Internet Key Exchange notification of INVALID_SELECTORS. 2. Establish communication through a security association with a designated host. 3. Send a packet inbound on the SA in which the packets headers are inconsistent with the selectors on the SA. 4. Verify that if the system has the ability to send an IKE notification of INVALID_SELECTORS enabled that the system receives a packet indicating that the message sent was discarded due to failure to pass selector checks. If the system has the ability to send an IKE notification of INVALID_SELECTORS disabled ensure that the system does not receive a packet indicating that the message sent was discarded due to failure to pass selector checks.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
73	**Section:** IP Security **ID:** 22.12 If RFC 4301 is supported, the system shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. The Encapsulating Security Payload is used to provide for Integrity, data origin authentication, and confidentiality in IPv4 and IPv6 environments. 2. Verify that ESP is being used by the system per RFC 4303 to provide secure communication.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4303			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
74	**Section:** IP Security **ID:** 22.12.1 If RFC 4303 is supported, the system shall be capable of enabling anti-replay. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4303	1. Ensure that the system supports Encapsulating Security Payload which provides anti-replay features for Security Associations. 2. Verify that the integrity feature is enabled for ESP as the anti-replay feature can not be enabled with out the integrity feature of ESP, because without the integrity service available the Sequence number field which is used to protect against anti-replay can not be checked for integrity. 3. Analyze network traffic sent from the security association and verify that the anti-replay service is in use.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
75	**Section:** IP Security **ID:** 22.12.2 If RFC 4303 is supported, the system shall check as its first check after a packet has been matched to its SA whether the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packet received during the life of the sec. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4303	1. Create a Security Association between two hosts on the test network. 2. After the SA has been created begin to generate traffic between the two hosts. 3. Verify that with each packet generated between the hosts that the counter for each packet is incremented. 4. If a sequence number between the hosts is duplicated it is an auditable event and the system will audit the event in its event log.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
76	**Section:** IP Security **ID:** 22.13 If RFC 4301 is supported, the system shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4308	1. Verify the system is capable of supporting the cryptographic algorithms for Suite VPN-B from RFC 4308. IPsec: Protocol: ESP ESP encryption: AES with 128-bit keys in CBC mode [AES-CBC] ESP integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] IKE and IKEv2: Encryption: AES with 128-bit keys in CBC mode [AES-CBC] Pseudo-random function: AES-XCBC-PRF-128 [AES-XCBC-PRF-128] Integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] Diffie-Hellman group: 2048-bit MODP	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
77	**Section:** IP Security **ID:** 22.13.1 If RFC 4301 is supported, the system shall support the use of AES-CBC with 128-bits keys for encryption. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Ensure the system is capable of supporting AES-CBC with 128-bit key for encryption. 2. Analyze network traffic between the system under test and a predetermined host to certify that it is using 128-bit encryption.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
78	**Section:** IP Security **ID:** 22.13.2 If RFC 4301 is supported, the system shall support the use of HMAC-SHA1-96 for (Threshold) and AES-XCBC-MAC-96 (FY2010). **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Confirm the test system is capable of supporting HMAC-SHA1-96 and AES-XCBC-MAC-96 for encryption. 2. Examine traffic between the system tested and another host on the network to confirm that HMAC-SHA1-96 and AES-XBC-MAC-96 is utilized for encryption.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
79	**Section:** IP Security **ID:** 22.14 If RFC 4301 is supported, the system shall support IKE Version 1 (IKEv1) (Threshold) as defined in RFC 2409, and IKE Version 2 (IKEv2) (FY2010) as defined in RFC 4306. NOTE: Internet Key Exchange version 1 (IKEv1) requirements are found in UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI(Softphone) Conditional: SS, NA, EBC, LS, EI	1. Create a Security Association between the system tested and another host on the test network. 2. Once the security association has been created begin to generate traffic between the hosts on the encrypted tunnel. 3. Verify that the request and response is created for the security association utilizing IKE and that the communication between the two hosts is encrypted properly. 4. The system must be capable of utilizing IKE and IKEv2 for secure communication.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
80	**Section:** IP Security **ID:** 22.14.1 If the system supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size. **Reference:** UCR 2008 5.3.5.3.9	Conditional: SS, NA, EBC, R, LS, EI	1. Confirm that the system is capable of supporting IKEv2. 2. Once you have verified that IKEv2 is utilized ensure that is capable of configuring UDP message size used for IKEv2. (i.e Although IKEv2 messages are intended to be short, they contain structures with no hard upper bound on size (in particular, X.509 certificates), and IKEv2 itself does not have a mechanism for fragmenting large messages. IP defines a mechanism for fragmentation of oversize UDP messages, but implementations vary in the maximum message size supported. Furthermore, use of IP fragmentation opens an implementation to denial of service attacks [KPS03]. Finally, some NAT and/or firewall implementations may block IP fragments. All IKEv2 implementations MUST be able to send, receive, and process IKE messages that are up to 1280 bytes long, and they SHOULD be able to send, receive, and process messages that are up to 3000 bytes long. IKEv2 implementations SHOULD be aware of the maximum UDP message size supported and MAY shorten messages by leaving out some certificates or cryptographic suite proposals if that will keep messages below the maximum. Use of the "Hash and URL" formats rather than including certificates in exchanges where possible can avoid most problems. Implementations and configuration should keep in mind, however, that if the URL lookups are possible only after the IPsec SA is established, recursion issues could prevent this technique from working.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			
81	**Section:** IP Security **ID:** 22.14.2 If IKEv2 is supported, the system shall support the use of the ID_IPv6_ADDR and ID_IPV4_ADDR Identification Type. **Reference:** UCR 2008 5.3.5.3.9.22.14.2	Conditional: SS, NA, EBC, R, LS, EI	1. Check the system under test to ensure that it is capable of supporting IKEv2. 2. Verify that the system is able to process both IPv4 and IPv6 addresses. 3. The ID_IPv6_ADDR and ID_IPv4_ADDR fields will be defined in the payload of the IKEv2 messages.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
82	**Section:** IP Security **ID:** 22.14.3 If the system supports IKEv2, the system shall be capable of ignoring subsequent SA setup response messages after the receipt of a valid response. **Reference:** UCR 2008 5.3.5.3.9	Conditional: SS, NA, EBC, R, LS, EI	1. Validate that the system tested has the ability to support IKEv2. 2. Certify that the system tested can create a security association between itself and another host. 3. Verify that the system receives a valid request and response to initially establish the security association. 4. Ensure that once the system has established the SA that any subsequent response messages pertaining to the request of the establishment of the SA is ignored rather than dropping the original security association and attempting to build a new one between the hosts.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
83	**Section:** IP Security **ID:** 22.14.4 If the system supports IKEv2, the system shall be capable of sending a Delete payload to the other end of the security association. **Reference:** UCR 2008 5.3.5.3.9	Conditional: SS, NA, EBC, R, LS, EI	1. Verify that the system under test supports IKEv2 2. Create a security association between the test system and a separate host. 3. Confirm the ability of the system tested to send a delete payload to the other end of the security association to terminate the SA.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
84	**Section:** IP Security **ID:** 22.14.5 If the system supports IKEv2, the system shall reject initial IKE messages unless they contain a Notify payload of type COOKIE. **Reference:** UCR 2008 5.3.5.3.9	Conditional: SS, NA, EBC, R, LS, EI	1. Ensure that the system tested is capable of using IKEv2 2. Attempt to send an initial IKE message to the system with a spoofed IP address and verify that the request is rejected. (e.g. An expected attack against IKE is state and CPU exhaustion, where the target is flooded with session initiation requests from forged IP addresses. This attack can be made less effective if a responder uses minimal CPU and commits no state to an SA until it knows the initiator can receive packets at the sending address. To accomplish this, a responder SHOULD -- when it detects a large number of half-open IKE_SAs -- reject initial IKE messages unless they contain a Notify payload of type COOKIE. It SHOULD instead send an unprotected IKE message as a response and include COOKIE Notify payload with the cookie data to be returned. Initiators who receive such responses MUST retry the IKE_SA_INIT with a Notify payload of type COOKIE containing the responder supplied cookie data as the first payload and all other payloads unchanged.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
85	**Section:** IP Security **ID:** 22.14.6 If the system supports IKEv2, the system shall close a SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: SS, NA EBC,R, LS,EI **Origin:** RFC 4306	1. Configure the system tested and the remote host with a basic IPv6 configuration. 2. Configure IKEv2 on both the system tested and remote host. 3. Create a Security Association between the two hosts with a preset lifetime for the SA. 4. Ensure that when the Security Association is created there is no traffic generated between the two hosts for this scenario. 5. Validate that when the lifetime expires that the system tested attempts to create a new Security Association rather than attempting to rekey the current session.	CAT II	
86	**Section:** IP Security **ID:** 22.14.7 If the system supports IKEv2, the system shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4306	1. Configure IKEv2 on the system tested. 2. Confirm that the system tested does not use EAP to authenticate. 3. Attempt to initiate IKE authentication using EAP with the system tested by having an initiator attempt to connect to the system tested with the request with AUTH payload absent from the inquiry. 4. Verify that the system tested does not respond back with the EAP payload accepting the request.	CAT II	
87	**Section:** IP Security **ID:** 22.14.8 If the system supports IKEv2, the system shall limit the frequency to which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4306	1. Attempt to send messages to the system tested with a separate host on UDP ports 500 and 4500. 2. The system shall not respond to a response message sent on UDP ports 500 and 4500 and must also audit the event. 3. The system may respond to a request message on these ports, if a response is sent it must be sent to the IP address and port from whence it came with the same IKE SPIs and the Message ID copied. The response MUST NOT be cryptographically protected and must contain a Notify payload indicating INVALID_IKE_SPI. 4. A node SHOULD treat such a message (and also a network message like ICMP destination unreachable) as a hint that there might be problems with SAs to that IP address and SHOULD initiate a liveness test for any such IKE_SA.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
88	**Section:** IP Security **ID:** 22.14.9 If the system supports IKEv2, the system shall not support temporary IP addresses or respond to such requests. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Create a security association with the system tested with the need of having the IP address of the system dynamically assigned to the system. 2. Confirm that the system does not support the ability to create this security association with the temporary IP address. 3. Also confirm that the system tested does not allow the system on the other end of the SA to allow for having a dynamic IP address.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
89	**Section:** IP Security **ID:** 22.14.10 If the system supports IKEv2, the system shall support the IKEv2 cryptographic algorithms defined in RFC 4307. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system supports IKEv2. 2. The system shall support the following algorithms defined in Section 3 of RFC 4307. **Encryption Algorithms** ENCR_3DES ENCR_NULL ENCR_AES_CBC ENCR_AES_CTR **Random Generating Algorithms** PRF_HMAC_MD5 PRF_HMAC_SHA1 PRF_AES128_CBC **Integrity Algorithms** AUTH_HMAC_MD5_96 AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4307			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
90	**Section:** IP Security **ID:** 22.14.11 If the system supports IKEv2, the system shall support the VPN-B Suite as defined in RFC 4308 and RFC 4869 (FY2010) **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Confirm that the system has the ability to support IKEv2. 2. Verify the system is capable of supporting the cryptographic algorithms for Suite VPN-B from RFC 4308. IPsec: Protocol: ESP ESP encryption: AES with 128-bit keys in CBC mode [AES-CBC] ESP integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] IKE and IKEv2: Encryption: AES with 128-bit keys in CBC mode [AES-CBC] Pseudo-random function: AES-XCBC-PRF-128 [AES-XCBC-PRF-128] Integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] Diffie-Hellman group: 2048-bit MODP 3. Also verify the system is capable of supporting the additional cryptographic algorithms for Suite VPN-B from Section 3 of RFC 4869.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4869			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
91	**Section:** IP Security **ID:** 22.15 If RFC 4301 is supported, the system shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 2407	1. Confirm the system tested provides support for ISAKMP. 2. Attempt to create a security association between the system tested and a separate host and verify the use of ISAKMP to negotiate that SA. 3. Verify the creation of the security association with ISAKMP and also ensure the encryption schemes defined in RFC 2407 are utilized.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
92	**Section:** IP Security **ID:** 22.16 If RFC 4301 is supported, the system shall support the ISAKMP as defined in RFC 2408. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 2408	1. Confirm the system tested provides support for ISAKMP. 2. ISAKMP is used to define procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). ISAKMP also defines payloads for exchanging key generation and authentication data. 3. Verify the systems use of ISAKMP while attempting to create a security association between the system tested and a separate host.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
93	**Section:** IP Security **ID:** 22.17 If the system supports the IPsec Authentication Header Mode, the system shall support the IP Authentication Header (AH) as defined in RFC 4302. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4302	1. Attempt to create a security association between the system tested and a separate host. 2. The system will need to support the authentication header which is used in secure communication between systems to provide connectionless integrity and data origin authentication, the authentication header also provides protection against replays. 3. Confirm its use by the system and analyze network traffic to see its use for outbound packets and the use of sequence numbering o the packets.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
94	**Section:** IP Security **ID:** 22.18 If RFC 4301 is supported, the system shall support manual keying of IPSec. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4301	1. Verify that the system under test has manual management techniques to employ statically configured, symmetric keys. 2. Verify the ability of the system to operate effectively after the manual keying.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
95	**Section:** IP Security **ID:** 22.19 If RFC 4301 is supported, the system shall support the ESP and AH cryptographic algorithm implementation requirements as defined in RFC 4305 and RFC 4835 (FY2010). **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system under test shall support the Encapsulating Security Payload and Authentication Header cryptographic algorithms which protect data sent being sent over a security association. 2. The cryptographic algorithms defined in RFC 4305 and RFC 4835 are as follows: **(ESP)** Requirement Algorithm ----------- ----------------------- **MUST** NULL **MUST** AES-CBC with 128-bit keys **MUST** TripleDES-CBC **SHOULD** AES-CTR **SHOULD NOT** DES-CBC **MUST** HMAC-SHA1-96 **SHOULD+** AES-XCBC-MAC-96 **MAY** NULL **MAY** HMAC-MD5-96 **(AH)** Requirement Algorithm ----------- ----------------------- **MUST** HMAC-SHA1-96 **SHOULD+** AES-XCBC-MAC-96 **MAY** HMAC-MD5-96	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4835 & RFC 4305			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
96	**Section:** IP Security **ID:** 22.21 If RFC 4301 is supported, the system shall support the IKEv1 security algorithms as defined in RFC 4109. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Check the system tested to confirm that it can support IKEv1. 2. The cryptographic algorithms defined in RFC 4109 are as follows: Requirement Algorithm ----------- ----------------------- **MAY** DES for Encryption **MUST** Triple DES for Encryption **SHOULD** AES-128 for Encryption **MAY** MD5 for Hashing and HMAC **MUST** SHA1 for Hashing and HMAC **MAY** Tiger for Hashing **SHOULD** AES-XCBC-MAC-96 for PRF **MUST** Preshared Secrets **SHOULD** RSA with signatures **MAY** DSA with Signatures **MAY** RSA for Encryption **MAY** D-H Group 1 (768) **MUST** D-H Group 2 (1024) **SHOULD** D-H Group 14 (2048) **MAY** D-H elliptical curves	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4109			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
97	**Section:** Network Management **ID:** 23 The system shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293. NOTE: The requirements to support SNMPv3 are found in UCR 2008, Section 5.3.2.17.3.1.5, SNMP Version 2 and Version 3 Format Alarm messages, and UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.10	Required: SS, NA, EBC, R, LS, EI	1. Verify the systems use of IPv6 and SNMP. 2. The system tested will need to conform to RFC 4293 for all of its MIBs for support of IPv6. 3. The changes defined in RFC 4293 for IPv6 are as follows: (There are several general classes of change that are required. -The first and most major change is that most of the previous objects have different object IDs and additional indexes to support the possibility of different address types. The general counters for IP and ICMP are examples of this. They have been moved to the ipSystemStatsTable and icmpMsgStatsTable, respectively. The second change is the extension of all address objects to allow for both IPv4 and IPv6 addresses and the addition of an address type object to specify what address type is in use. The third change is the addition of several new objects to the replacement for a previously existing table such as IpNetToPhysical. The fourth change is the addition of completely new tables such as ipIfStatsTable and ipDefaultRouterTable. The first is based on the previous statistics groups, while the second is completely new to this MIB.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4293			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
98	**Section:** Network Management **ID:** 23.1 If the system performs routing functions, the system shall support the SNMP management framework as described in RFC 3411. **Reference:** UCR 2008 5.3.5.3.10	Required: LS	1. Verify that the system under test will support SNMP management framework. 2. Ensure several (potentially many) nodes, each with an SNMP entity containing command responder and notification originator applications, which have access to management instrumentation (traditionally called agents). 3. Verify at least one SNMP entity containing command generator and/or notification receiver applications (traditionally called a manager) 5. Verify management protocol, used to convey management information between the SNMP entities.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3411			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
99	**Section:** Network Management **ID:** 23.2 If the system performs routing functions, the system shall support SNMP message processing and dispatching as described in RFC 3412. **Reference:** UCR 2008 5.3.5.3.10	Required: LS	1. Verify that the system currently supports SNMP. 2. The system that supports SNMP must follow RFC 3412 for message processing and dispatching of SNMP. 3. The dispatcher in SNMP sends and receives the messages in SNMP and also dispatches SNMP PDU's to SNMP applications. 4. The message processor is responsible for processing SNMP version-specific messages and coordinating the interaction with the security subsystem to ensure proper security is applied to the SNMP message being handled.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3412			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
100	**Section:** Network Management **ID:** 23.3 If the system performs routing functions, the system shall support the SNMP applications as described in RFC 3413. **Reference:** UCR 2008 5.3.5.3.10	Required: LS	1. Confirm that the system has the ability to supports SNMP applications defined in RFC 3413. 2. RFC 3413 currently defines the following five types of SNMP application in which the system tested will need to support. - Applications which initiate SNMP Read-Class, and/or Write-Class requests, called 'command generators.' - Applications which respond to SNMP Read-Class, and/or Write-Class requests, called 'command responders.' - Applications which generate SNMP Notification-Class PDUs, called 'notification originators.' - Applications which receive SNMP Notification-Class PDUs, called 'notification receivers.' - Applications which forward SNMP messages, called 'proxy forwarders.' 3. Verify that the system tested shows the ability to support each of these SNMP applications.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3413			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
101	**Section:** Network Management **ID:** 24 The system shall support the ICMPv6 MIBs as defined in RFC 4293. **Reference:** UCR 2008 5.3.5.3.10	Required: SS, NA, EBC, R, LS	1. Confirm that the system tested if currently utilizing ICMPv6 MIBs. 2. The system is to support ICMPv6 MIBs defined in RFC 4022. 3. The system under test will need to support the addition of the ipSystemStatsTable and ipIfStatsTable tables which specify IP address type in order to separate information based on IP versions. 3. The system will also have the need to support tables, such as ipDefaultRouterTable, which may be useful on both IPv4 and IPv6 nodes and also ipv6RouterAdvertTable.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4293			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
102	**Section:** Network Management **ID:** 25 The system shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022. **Reference:** UCR 2008 5.3.5.3.10	Required: SS, NA, EBC, R, LS	1. Confirm that the system tested is currently utilizing TCP MIB. 2. The system is to support TCP MIBs defined in RFC 4022. 3. TCP MIBs defined in RFC 4022 includes a group of scalars and two tables which are the following: The tcp group of scalars includes two sets of objects: -Parameters of a TCP protocol engine. These include parameters such as the retransmission algorithm in use (e.g., vanj [VANJ]) and the retransmission timeout values. -Statistics of a TCP protocol engine. These include counters for the number of active/passive opens, input/output segments, and errors. Discontinuities in the stats are identified identified via the sysUpTime object, defined in [RFC 3418]. -The tcpConnectionTable provides access to status information for all TCP connections handled by a TCP protocol engine. In addition, the table reports identification of the operating system level processes that handle the TCP connections. -The tcpListenerTable provides access to information about all TCP listening endpoints known by a TCP protocol engine. And as with the connection table, the tcpListenerTable also reports the identification of the operating system level processes that handle this listening TCP endpoint.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4022			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
103	**Section:** Network Management **ID:** 26 The system shall support the UDP MIBs as defined in RFC 4113. **Reference:** UCR 2008 5.3.5.3.10	Required: SS, NA, EBC, R, LS	1. Confirm that the system tested if currently utilizing UDP MIBs. 2. The system is to support UDP MIBs defined in RFC 4113. 3. UDP MIBs defined in RFC 4113 includes a group of scalars and one table which are the following: The current UDP-MIB consists of one table and a group of scalars: -The udp group of scalars reports parameters and statistics of a UDP protocol engine. Two scalars, udpHCInDatagrams and udpHCOutDatagrams, have been added to this group since the publication of RFC 2013 in order to provide high-capacity counters for fast networks. Discontinuities in the values of the counters in this group are indicated by discontinuities in the value of the sysUpTime object, which is defined in RFC 3418 -The udpEndpointTable provides access to status information for all UDP endpoints handled by a UDP protocol engine. The table provides for strictly listening endpoints, as with the historical udpTable, and also for "connected" UDP endpoints, which only accepts packets from a given remote system. It also reports identification of the operating system level processes that handle UDP connections. Addresses and ports of UDP endpoints in this table are represented using the InetAddressType, InetAddress, and InetPortNumber textual conventions defined in RFC 4001.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4113			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
104	**Section:** Network Management **ID:** 27 If the system performs routing functions, the system shall support IP tunnel MIBs as described in RFC 4087. **Reference:** UCR 2008 5.3.5.3.10	Required: LS	1. Ensure that the system tested can support IP tunnel MIBs. 2. The system is to support IP tunnel MIBs which are defined in RFC 4113. 3. IP tunnel MIBs defined in RFC 4087 includes two current tables. The current tables are: -The Tunnel Interface Table, containing information on the tunnels known to a router; and -The Tunnel Inet Config Table, which can be used for dynamic creation of tunnels, and also provides a mapping from endpoint addresses to the current interface index value.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4087			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
105	**Section:** Network Management **ID:** 28 If the system performs routing functions, the system shall support the IP Forwarding MIB as defined in RFC 4292. **Reference:** UCR 2008 5.3.5.3.10	Required: LS	1. Confirm that the system under test may process IP Forwarding MIBs. 2. The system is to support IP Forwarding MIBs which are defined in RFC 4292. 3. IP Forwarding MIBs defined in RFC 4292 includes one current table and two global objects: -The object inetCidrRouteNumber indicates the number of current routes. This is primarily to avoid having to read the table in order to determine this number. -The object inetCidrRouteDiscards counts the number of valid routes that were discarded from inetCidrRouteTable for any reason. This object replaces the ipRoutingDiscards and ipv6DiscardedRoutes objects. -The inetCidrRouteTable provides the ability to display IP version-independent multipath CIDR routes.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4292			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
106	**Section:** Network Management **ID:** 29 If the system supports mobile users, the system shall support the Mobile IP Management MIBs as described in RFC 4295. **Reference:** UCR 2008 5.3.5.3.10	Required: R, LS	1. Check the system being tested to verify that it may use Mobile IP Management MIBs. 2. The system is to support Mobile IP Management MIBs which are defined in RFC 4295. 3. Mobile IP Management MIBs defined in RFC 4295 includes: -It is assumed that the Mobile IPv6 Management Information Base (MOBILEIPV6-MIB) will always be implemented in conjunction with the IPv6-capable version of the IP-MIB. The MOBILEIPV6-MIB uses the textual conventions defined in the INET-ADDRESS-MIB. The Mobile-IPv6 MIB is composed of the following groups of definitions: - mip6Core: a generic group containing objects that are common to all the Mobile IPv6 entities. - mip6Ha: this group models the home agent service. It is composed of objects specific to the services and associated advertisement parameters offered by the home agent on each of its links. It also contains objects pertaining to the maintenance of the home agent list on each of the	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4295			

Table E-7. IPv6 Requirements (continued)

106 (continued)			links on which the service is offered. - mip6Mn: this group models the mobile node service. It is composed of objects specific to the Dynamic Home Agent discovery function and related parameters. It also contains objects that record the movement of the mobile node. - mip6Cn: models the correspondent node and is primarily scoped to its participation in the Return Routability procedure for achieving Route Optimization triggered by the mobile node. - mip6Notifications: defines the set of notifications that will be used to asynchronously monitor the Mobile IPv6 entities. The tables contained in the above groups are as follows: -mip6BindingCacheTable: models the binding cache on the home agent and correspondent node. It contains details of the Binding Update requests that have been received and accepted. -mip6BindingHistoryTable: tracks the history of the binding cache. -mip6NodeTrafficTable: the mobile node-wise traffic counters. -mip6MnHomeAddressTable: contains all the home addresses pertaining to the mobile node and the corresponding registration status. -mip6MnBLTable: models the Binding Update List on the mobile node. It contains information about the registration requests sent by the mobile node and the corresponding results. -mip6CnCounterTable: contains the mobile node-wise registration statistics. -mip6HaConfTable: contains the configurable advertisement parameters for all the interfaces on which the home agent service is advertised. -mip6HaCounterTable: contains registration statistics for all mobile nodes registered with the home agent.			

Table E-7. IPv6 Requirements (continued)

106 (continued)			-mip6HaListTable: contains the list of all routers that are acting as home agents on each of the interfaces on which the home agent service is offered by this router. -mip6HaGlAddrTable: contains the global addresses of the home agents.		

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
107	**Section:** Network Management **ID:** 31 If the system supports SNMP and IPsec, the system shall support the IPsec security policy database as described in RFC 4807. **Reference:** UCR 2008 5.3.5.3.10	Required: LS	1. Confirm support for the Management Information Base (MIB) module for configuring the security policy database of a device implementing the IPsec protocol. 2. The system shall conform to the requirements listed in RFC 4807 for support of the IPSec security policy: (i.e. The Distributed Management Task Force (DMTF) has created an object oriented model of IPsec policy information known as the IPsec Policy Model White Paper [IPPMWP]. The "IPsec Configuration Policy Model" (IPCP) [RFC 3585] is based, in large part, on the DMTF's IPsec policy model and on RFC 2401. The IPCP document describes a model for configuring IPsec. This MIB module is a task-specific derivation (i.e., an SMIv2 instantiation) of the IPCP's IPsec configuration model for use with Simple Network Management Protocol version 3 (SNMPv3). The high-level areas where this MIB module diverges from the IPCP model are: -Policies, Groups, Conditions, and some levels of Actions are generically named. In other words, IPsec-specific prefixes like "SA" (Security Association), or "IPsec", are not used. This naming convention is used because packet classification and the matching of conditions to actions is more general than IPsec. The tables in this document can possibly be reused by other packet-transforming actions, which need to conditionally act on packets matching filters. -Filters are implemented in a more generic and scalable manner, rather than enforcing the condition/filtering pairing of the IPCP and its restrictions upon the user. This MIB module offers a compound filter object providing greater flexibility for complex filters than the IPCP.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4807			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
108	**Section:** Network Management **ID:** 32 If the system uses Uniform Resource Identifiers (URIs), the system shall use the URI syntax described in RFC 3986. **Reference:** UCR 2008 5.3.5.3.10	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system uses Uniform Resource Identifiers for the identifying resources on the network which is essentially a resource locator. 2. The syntax for URI defined in RFC 3896 is as follows: The generic URI syntax consists of a hierarchical sequence of components referred to as the scheme, authority, path, query, and fragment. URI = scheme ":" hier-part ["?" query] ["#" fragment] hier-part = "//" authority path-abempty / path-absolute / path-rootless / path-empty	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3986			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
109	**Section:** Network Management **ID:** 33 If the system uses the Domain Name System (DNS), the system shall conform to RFC 3596 for DNS queries. NOTE: DNS is primarily used for NM applications. **Reference:** UCR 2008 5.3.5.3.10	Required: SS, NA, EBC, R, LS, EI	1. Confirm that the system is using Domain Name System for IPv6. 2. DNS is unable to support IPv6 addresses unless it conforms to the requirements in RFC 3596. (i.e. Current support for the storage of Internet addresses in the Domain Name System (DNS) cannot easily be extended to support IPv6 addresses since applications assume that address queries return 32-bit IPv4 addresses only. To support the storage of IPv6 addresses in the DNS, RFC 3596 defines the following extensions: -A resource record type is defined to map a domain name to an IPv6 address. -A domain is defined to support lookups based on address. -Existing queries that perform additional section processing to locate IPv4 addresses are redefined to perform additional section processing on both IPv4 and IPv6 addresses.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3596			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
110	**Section:** IP Version Negotiation **ID:** 37 The system shall forward packets using the same IP version as the version in the received packet. NOTE: If the packet was received as an IPv6 packet, the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur. REMINDER: This requirement may be waived from FY2008 to FY2012 in order to support IPv4 or IPv6 only EIs. **Reference:** UCR 2008 5.3.5.3.12	Required: SS, EBC	1. Send packets to the system under test with both an IPv4 and IPv6 system on the test network. 2. Verify that when the packets are received by the system tested from either the IPv4 or IPv6 system that the packet forwarded uses the same IP version as the packet that was received.	CAT II	
	IA Control: ECSC-1	**Origin:** Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
111	**Section:** IP Version Negotiation **ID:** 38 The system shall use the Alternative Network Address Types (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091 when establishing media streams from dual stacked appliances for AS-SIP signaled sessions. **Reference:** UCR 2008 5.3.5.3.12	Required: SS, NA, EI	1. Confirm that the system under test has the capability of providing Alternative Network Address Types for the Session Description Protocol. 2. Attempt to create a request for ANAT with the system tested and a dual stacked appliance. 3. Confirm that the system is offered the use of both an IPv6 and an IPv4 address. 4. The system tested shall choose the one set of addresses to create a single logical media stream for communication with the dual stacked appliance.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4091			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
112	**Section:** IP Version Negotiation **ID:** 38.2 The system shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092. **Reference:** UCR 2008 5.3.5.3.12 **IA Control**: ECSC-1	Required: SS, NA, EI **Origin:** RFC 4091 and RFC 4092	1. Attempt to solicit a request for the use of an Alternative Network Address Type (ANAT) to a separate system. 2. Verify that the SDP-ANAT option-tag is placed in the header-field when sending the ANAT request. 3. The SDP-ANAT option tag is used to verify that the recipient of the offer to use ANAT in fact supports its use, in which case it does not support its use the SDP-ANAT header can be used to ensure that an offer using ANAT is not processed by answerers without support for ANAT. The option-tag can also be used to explicitly discover the capabilities of a UA (i.e., whether it supports ANAT).	CAT II	
113	**Section:** IP Version Negotiation **ID:** 38.3 Dual stacked systems shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP. **Reference:** UCR 2008 5.3.5.3.12 **IA Control:** ECSC-1	Required: EI **Origin:** RFC 4091	1. Verify session establishment and the exchanging of the SDP between the system tested and a separate host. 2. Confirm that IPv4 and IPv6 addresses and located within the SIP INVITE.	CAT II	
114	**Section:** AS-SIP IPv6 Unique Requirements **ID:** 45 The system shall be able to provide topology hiding (e.g., NAT) for IPv6 packets in the manner described in UCR 2008 Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.13 **IA Control**: ECSC-1	Required: EBC **Origin:** UCR 2008 Section 5.4	1. Confirm the system tested has the ability to provide topology hiding for IPv6 addresses. 2. Topology Hiding can be accomplished in a number of different ways in Section 5.4.5.4.7 Edge Boundary Control Appliances in UCR 2008 it talks about the use of private addressing in IPv6 for the function of topology hiding. 3. Verify from outside the test network that you do not have the ability to map out the IP addresses used within the test network.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
115	**Section:** AS-SIP IPv6 Unique Requirements **ID:** 46 The system shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1). **Reference:** UCR 2008 5.3.5.3.13	Required: EI (Softphone)	1. Validate that the system tested has the ability to process the algorithms defined in RFC 3484 to complete default address selection to communicate with IPv6 hosts. . (i.e. The IPv6 addressing architecture allows multiple unicast addresses to be assigned to interfaces. These addresses may have different reachability scopes (link-local, site-local, or global). These addresses may also be "preferred" or "deprecated". Privacy considerations have introduced the concepts of "public addresses" and "temporary addresses". The mobility architecture introduces "home addresses" and "care-of addresses". In addition, multi-homing situations will result in more addresses per node. For example, a node may have multiple interfaces, some of them tunnels or virtual interfaces, or a site may have multiple ISP attachments with a global prefix per ISP. The end result is that IPv6 implementations will very often be faced with multiple possible source and destination addresses when initiating communication.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3484			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
116	**Section:** Miscellaneous Requirements **ID:** 47 If the system supports Remote Authentication Dial In User Service (RADIUS) authentication, the system shall support RADIUS in the manner defined in RFC 3162. **Reference:** UCR 2008 5.3.5.3.13	Required: EBC, R, LS	1. Conduct an analysis of the system. 2. Verify accuracy of diagrams delineating each component, operating system, firmware version, application version, and test boundaries. Make a connection through RADIUS to both an IPv6 and IPv4 system.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3162			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
117	**Section:** Miscellaneous Requirements **ID:** 48 If the system supports Mobile IP version 6 (MIPv6), the system shall provide mobility support as defined in RFC 3775. **Reference:** UCR 2008 5.3.5.3.14	Required: EI (Softphone)	1. Check the system to confirm that has the capability to utilize Mobile IP version 6. 2. Attempt to setup the system on the test network to support Mobile IP version 6. 3. Take note of the home address of the system as this is what will be used to communicate with the host. 4. Connect the host to a separate segment on the test network and attempt to bind the care-of-address from the separate segment to the home agent to route source packets for the test system. 5. Verify that you are able to communicate with the system while it is on its normal link via its home address and you are able to communicate with the system while it is on a separate network segment via its care-of-address.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3775			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
118	**Section:** Miscellaneous Requirements **ID:** 48.1 If the system acts as a home agent, the system shall provide mobility support as defined in RFC 3775. **Reference:** UCR 2008 5.3.5.3.14	Required: R	1. Validate that the system has the ability to act as a home agent. 2. Verify that once the system is setup as a home agent that you configure a separate host on the network to work as a mobile node. 3. Confirm that the host registers its home address with the home agent to allow it to bind its car-of-address once taken off of the local network to its home address to allow for the home agent to provide mobility support. 4. Remove the separate host from the local network segment and attach it to another segment, verify that it sends a binding update to the test system. 5. Attempt to communicate with the host on the separate network segment and ensure that the system tested routes the traffic to the mobile host.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3775			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
119	**Section:** Miscellaneous Requirements **ID:** 49 If the system supports Mobile IP version 6 (MIPv6), the system shall provide a secure manner to signal between mobile nodes and home agents in manner described in RFC 3776 and RFC 4877 (FY2010). **Reference:** UCR 2008 5.3.5.3.14	Required: R, EI (Softphone)	1. The system tested shall have the ability to support Mobile IP version 6. 2. The home agent should check if a particular mobile node is authorized to use a home address before creating an IPSec security association. 3. The system shall have the ability to verify through the SPD the binding update of either a mobile node or a home agent. 4. The home agent then may store the assigned home address in the SPD entries created for a mobile node.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4877			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
120	**Section:** Miscellaneous Requirements **ID:** 51 If the system supports network mobility (NEMO), the system shall support the function as defined in RFC 3963. **Reference:** UCR 2008 5.3.5.3.14	Required: R, EI (Softphone)	1. Confirm the existence of the mobile network and also a mobile router for support of that network. 2. Setup the mobile router on the test network in place to register its home address on the local network with a local router. 3. Connect the router to a separate network segment and configure it to support the mobile network configured. 4. Confirm that the mobile router sends a binding update back to the local system on the original network where its home address is registered on and that the mobile router sends the binding update with its new care-of-address. 5. Verify that you are able to communicate with the system while it is on its normal link via its home address and you are able to communicate with the mobile network while it is on a separate network segment via its care-of-address.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3963			

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
121	**Section:** Miscellaneous Requirements **ID:** 52 The systems shall support Differentiated Services as Described in RFC 2474 and RFC 5072 (FY 2010) for a voice and video stream to the security association in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements and UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan. **Reference:** UCR 2008 5.3.5.3.14 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 5072	1. Ensure the system has the ability to support the use of differentiated services in accordance with RFC 2474 and RFC 5072. 2. Setup a security association between the test system and a separate host on the network. 3. Make sure that for that security association of the two systems that you have a voice and video system configured for use. 4. Begin to generate traffic to communicate with the voice and video system. 5. Analyze traffic on the network to confirm that the system is properly forwarding packets and is also differentiating between the voice and video packets 6. Also verify that the system is allowing for the ability to configure parameters for the differential treatment for the care of the different services of the network traffic.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
122	**Section:** Miscellaneous Requirements **ID:** 53 If the system acts as an IPv6 tunnel broker, the system shall support the function in the manner defined in RFC 3053. **Reference:** UCR 2008 5.3.5.3.14 **IA Control:** ECSC-1	Required: EI (Softphone) **Origin:** RFC 3053	1. Ensure that the system has the ability to act as an IPv6 tunnel broker. 2. Once it is verified that the system has the ability to act as a tunnel broker you will need to place it on the test network. 3. Once placed on the test network configure a tunnel to allow for access by a preconfigured IPv6 host already on the test network. 4. Verify that the host on the network has the ability to tunnel through the system under test to communicate with a preconfigured IPv4 test network through the use of the tunnel broker.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
123	**Section:** Miscellaneous Requirements **ID:** 54 If the system supports roaming (as defined within RFC 4282), the system shall support this function as described by RFC 4282. **Reference:** UCR 2008 5.3.5.3.14 **IA Control**: ECSC-1	Required: R **Origin:** RFC 4282	1. Configure the system under test to have the ability to have a secure VPN communication between itself and a host. 2. Per RFC 4282 there are a number of means for a system to comply with roaming. 3. The user of the system must first have a Network Access Identifier to identify themselves to authenticate with the Network Access Server. 4. Once the user has authenticated to the Network Access Server through the Network Access Identifier then he will have the ability to open a tunnel for secure access to a VPN.	CAT II	

Table E-7. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
124	**Section:** Miscellaneous Requirements **ID:** 55 If the system supports the Point-to-Point Protocol (PPP), the system shall support PPP as described in RFC 2472. **Reference:** UCR 2008 5.3.5.3.14	Required: R	1. Verify the system under test is capable of supporting the Point-to-Point Protocol. 2. Attempt to create a Point-to-Point connection between the system under test and another host on the test network. 3. Ensure that the system tests the connection and ensures it is available and that PPP reaches the network-layer protocol phase. 4. Once both sides have verified the connection view communication between the hosts until one side explicitly closes the connection.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2472			

LEGEND:

AES	Advanced Encryption Standard
AH	Authentication Header
ANAT	Alternative Network Address Types
AS-SIP	Assured Services Session Initiation Protocol
BGP	Border Gateway Protocol
CAT	Category
CBC	Cipoher Block Chaining
CE	Customer Edge
CPU	Central Processing Unit
DCBP	Design Configuration Best Practices
DCSP	Design Configuration System
DHCP	Domain Host Control Protocol
DMTF	Distributed Management Task Force
DNS	Domain Name Service
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EBC	Edge Border Controller
ECSC	Enclave Computing Environment Security Configuration Compliance
EI	End Instrument
ESP	Encapsulating Security Payload
EUI	Extended Unique Identifier
FY	Fiscal Year
HMAC	Hashed Message Authentication Code
IA	Information Assurance
ICMP	Internet Control Message Protocol
ID	Identification
IKE	Internet Key Exchange
IP	Internet Protocol
IPCP	IPsec Configuration Policy
IPSEC	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LS	LAN Switch
MAC	Media Access Control
MIB	Management Information Base
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
MFS	Multifunction Softswitch
NA	Network Appliance
NAT	Network Address Translation
NIC	Network Interface Card
OSPF	Open Shortest Path First
PC	Personal Computer
PDU	Protocol Data Unit
PMTU	Path Maximum Transmission Unit
PPP	Point-to-Point Protocol
R	Revision
R	Router
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
SA	Security Association
SAD	Security Association Database
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
SPI	Security Parameter Index
SS	Softswitch
STIG	Security Technical Implementation Guidelines
TCP	Telecommunications Protocol
UA	User Agent
UC	Unified Capabilities
UCR	Unified Capabilities Requirement
UDP	User Datagram Protocol
URI	Uniform Resource Identifiers
V	Version
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VVoIP	Video and Voice over Internet Protocol
VLAN	Virtual Local Area Network

3. Post Test. An IA Assessment Draft Findings Report is generated using the findings that were annotated in the DIACAP Scorecard. The vendor provides feedback and mitigations for any findings that could not be resolved during testing. At this time an out-brief is scheduled to discuss the report and the vendor's mitigations.

E-2. INTERNET PROTOCOL (IP) VULNERABILITY TESTING/PROTOCOL ANALYSIS (PA)

1. Background. The GNTF's mission is to enhance the product's IA posture and readiness, as well as their Defense-in-Depth strategy. The Joint Interoperability Test Command (JITC) conducts vulnerability assessments and penetration testing on vendors' products before undergoing Interoperability certification. Program Managers or DoD agencies must obtain IA accreditation on new telecommunication equipment for which DSN connectivity is planned or for existing DSN telecommunication equipment that has planned upgrades, systems that are Unified Capabilities, and the Real Time Services systems. The IP Vulnerability (IPV) testing is conducted in accordance with the recommendations contained in the National Institute of Standards and Technology (NIST) Special Publication 800-42: "Guideline on Network Security Testing." The system will be evaluated for its ability to maintain confidentiality, integrity, and availability derived from Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

2. Purpose. The purpose of the IPV Testing/PA Standard Operating Procedure is to provide a consistent set of guidelines to address Information Technology (IT) hardware and software for testers and lab personnel. The purpose is also to aid the testers in executing these tasks related to the maintenance of hardware and software, as well as default usage and finding documentation. A penetration test is designed to simulate an inside and/or an outside attack. These test scenarios are outlined by the Initial Contact Meeting, but can change to reflect the Deployment Configuration of the System Under Test (SUT).

3. Preparation. Before starting an assessment, test personnel will acquire the latest patches for their test tools from a designated "dirty" network drop connection. Testers will acquire their patches only from the vendor website or from the IA update and backup server. The team will not connect the IPV laptops, PA laptops, "Lab Only" thumb drives to the DISA computers, or DISA Local Area Network (LAN) drops. A back-up image with a default load of approved applications is located on the IA backup server and updated with a quarterly update interval.

4. Roles and Responsibilities. Penetration testing is conducted by personnel designated by the IA Task Manager as a minimum of Information Assurance Technical (IAT) Level II certified by DoD 8570.01-M standards. The IAT Level II personnel provide Network Environment and advanced level Customer Equipment support to the GNTF. They pay special attention to detecting intrusion, finding and fixing unprotected vulnerabilities, and ensuring that remote access points are well secured. These positions focus on threats and vulnerabilities and improve the security of systems. The

IATT Level II personnel have mastered the methods of gaining access to a system by using common tools and techniques used by malicious users.

5. Functionality Test Procedures. The first step in performing a vulnerability test is to perform a functionality check. Testing the SUT's functionality ensures that the product operates as intended in a fielded environment. Perform the functionality test at the beginning of Phase II testing to ensure that all services and applications are functioning and communicating correctly. Functionality testing varies from system to system and targets the basic operational functions. It is not a substitute for an interoperability test.

Some products, such as the Customer Premise Equipment, rely on external systems to exercise their capabilities. For example, a secure modem solution is inactive until an external switch initiates a call. In this case, the external switch is outside the scope of the IA test. However, the tester and vendor must ensure the external switch is operational in order to perform IPV testing on the secure modem solution. Functionality tests are performed before Phase II testing begins, and then again at the conclusion of Phase II testing. Monitor IP Traffic during the functionality and save the results for further evaluation. The objective is to ensure that the SUT is functionally operational before Phase II IPV testing commences.

The IPV testing should be performed from the external or outside perspective and from the internal or inside perspective. An inside perspective is analogous to what a "trusted insider" or an employee has, or the same as an attacker would have once perimeter defenses (firewalls) are breached. An outside perspective is analogous to the same perspective someone would have on the Internet, looking in at the system. The attacker would have the perspective of an "untrusted outsider" and would be looking in at the product. The following DoDI 8500.2 IA Controls apply to all the IPV testing procedures: DCPP-1, ECVI-1, ECTM-2, VIVM-1, and ECMT-1.

6. Internet Protocol (IP) Interface Identification. Verify operational functionality and identify all IP interfaces.

a. Lines. If the SUT supports lines, the following manual calls are attempted: Analog to Analog, IP to IP, Analog to IP, and IP to Analog. Verify that all test calls can be completed successfully.

b. Trunks. If the SUT supports trunks, the following manual calls are attempted: Analog over trunk, IP over trunk. Verify that all test calls can be completed successfully.

c. Internet Protocol Handsets. All IP handsets are identified, and the protocols used identified (e.g., Session Initiation Protocol (SIP) and Simple Client Control Protocol (SCCP)).

7. System Under Test (SUT) Test Procedures.

a. Test Perspectives. The IPV and PA testing are performed from an external and internal perspective. An external perspective is what someone on the Internet, DISA Network, or Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) would see from outside the network (i.e., an attacker looking in at the network's outer perimeter defenses, such as a firewall and/or router with an ACL). An internal perspective is what someone would see from inside the system (i.e., a trusted employee, a client user, or an attacker who has breached the firewalls). This method of testing can be found in section 3 of the NIST Special Publication 800-42, Guideline on Network Security Testing. The following Department of Defense Instruction (DoDI) 8500.2 IA Controls apply to all of the IPV testing procedures: DCPP-1, ECVI-1, ECTM-2, VIVM-1, and ECMT-1.

b. Host Discovery. Detecting all possible hosts in use of the SUT and their corresponding IP address information is the first step in the technical evaluation process. Although the product vendor provides the IP address information, the test team ensures that there are no other undocumented IP-routable addresses. In addition to the physical host network adapters, an IP address can be discovered from a variety of sources. Such sources include virtual Ethernet adapters, virtual machine addresses, and host-based network addresses, which can create vulnerabilities in the SUT. The following are general techniques that are used to discover available hosts or other IP-routable end-points.

(1) Ping Sweep. A general Packet Internet Groper (Ping) sweep determines what hosts are available through the Internet Control Message Protocol (ICMP) message. This is generally an ICMP echo request (type 8) to elicit an ICMP echo reply (type 0) from a host.

Table E-8 shows the Ping sweep test procedures, which use the following testing components: a laptop with a port scanning application installed, a laptop assigned with an IP address compliant with the test environment, and an Ethernet hub.

Table E-8. Ping Sweep Test Procedures

Procedure	Results
Configure IP vulnerability testing laptop. Ethernet connection: An Ethernet port on the SUT, with its associated IP address, should be available for test purposes. The port location should be such that access to the largest number of IP addresses within the solution is possible. Use of an Ethernet hub is the preferred method of connection.	The IP test laptop and the IP interfaces under test are cabled to the Ethernet hub.
Assign IP address: An IP address and Subnet mask will be assigned to the laptop NIC that is within the range being used by the SUT.	The IP test laptop is configured with an IP address that is included within the Subnet range of the SUT. The use of the "Ping" command verifies that the test laptop can communicate with the SUT.

Table E-8. Ping Sweep Test Procedures (continued)

Procedure	Results
Host Discovery: A general ICMP (Ping) sweep of the entire subnet will be conducted to discover any devices within the SUT that respond to an ICMP. The following is an example of a ping sweep of a standard class C IP address range using NMAP: #NMAP –sP –n 192.168.1.1-254	The results returned by the ICMP Ping sweep will include all available hosts within the subnet.
Eliminate “out of bounds” components: Items such as gateways, network elements, or end-points that are outside the IA test boundary will be removed from the discovery findings and a list of discovered hosts will be established.	An evaluation of the returned results will eliminate all components that are considered “out of the test boundary” for the SUT.

LEGEND:

IA	Information Assurance	NMAP	Networked Messaging Application Protocol
ICMP	Internet Control Message Protocol	Ping	Packet Internet Groper
IP	Internet Protocol	SUT	System Under Test
NIC	Network Interface Card		

(2) Transmission Control Protocol (TCP) Sweep. A TCP sweep provides insight into available hosts when the ICMP is disabled. A TCP sweep attempts to make TCP connections to a host range on a specified port list. In the process of the TCP sweep, a “three-way handshake” happens. The originator sends an initial packet called a Synchronous (SYN) to establish communication and "synchronize”. The destination then sends a “SYN/Acknowledge (ACK)” which again “synchronizes” with the originator and acknowledges the initial packet. The originator then returns an “ACK” which acknowledges the packet the destination just sent him. The connection is now “OPEN” and ongoing communication between the originator and the destination are permitted until one of them issues a Finish (FIN) packet, or a Reset (RST) packet, or the connection times out. The "three-way handshake" establishes the communication.”

By providing a list of possible ports that might be available within a system or product, the TCP connections are able to determine which hosts are up and available. Common ports used in TCP sweeps include (but are not limited to) 21, 22, 23, 25, 54, 80, 137, 139, 443, and 445. Table E-9 shows the TCP sweep test procedures, which use the following components: a laptop with a port scanning application installed, a laptop assigned with an IP address compliant with the test environment, and an Ethernet hub.

Table E-9. TCP Sweep Test Procedures

Procedure	Results
Host Discovery: A TCP sweep of the IP address space will be conducted to discover devices that are not responding to ICMP or might be using host-based firewalls or IDSs. The following is an example of a TCP ping sweep (System Ping) of a standard class C IP address range using NMAP: # NMAP –PS –p1-65000 192.168.1.1-254	The results returned by the TCP sweep will include all available hosts within the subnet that did not respond to the ping sweep.
Eliminate “out of bounds” components: The list of hosts that responds to this sweep will be compared to the list of hosts defined in the ICMP sweep and any newly discovered host will be added to the list of known hosts.	An evaluation of the returned results will eliminate all components that are considered “out of bounds” for this test.

Table E-9. TCP Sweep Test Procedures (continued)

Procedure	Results
Additional Hosts: At this point, if the test team is satisfied that all the hosts are discovered, they could move to traffic analysis or they could utilize ACK scans, ARP scans, or alternate ICMP scans using different ICMP types.	Any additional hosts discovered should be confirmed to be part of the SUT.

LEGEND:

ACK	Acknowledge	IP	Internet Protocol
ARP	Address Resolution Protocol	NMAP	Networked Messaging Application Protocol
ICMP	Internet Control Message Protocol	SUT	System Under Test
IDS	Intrusion Detection System	TCP	Transmission Control Protocol

(3) Traffic Analysis. Traffic analysis allows the test team to determine all the hosts that the SUT uses in an operational environment. Accessing the network traffic in transit provides an in-depth look at how information flows within the application and can also be helpful in revealing hosts that are part of the communications process. This process may require placing a network hub within the environment, network traffic flow, or possibly in the configuration of a mirror port on an existing network element. Table E-10 shows the traffic analysis test procedures, which use the following testing components: a laptop with a port scanning application installed, a laptop assigned with an IP address compliant with the test environment, and an Ethernet hub.

Table E-10. Traffic Analysis Test Procedures

Procedure	Results
Initialize Traffic Sniffer: A network analyzer such at *WireShark* (Ethereal) or *tcpdump* would be enabled in order to view all the network traffic and ensure that data was not traveling to devices that were not detected by the scanning and sweeping methods.	Confirm that all network traffic being generated and passed is between components of the SUT only.
Additional Hosts: If any new hosts are discovered during the traffic analysis phase of testing, they will be added to the list of auditable end-points, generally in a text file for the Phase II evaluation.	Any additional hosts discovered should be confirmed to be part of the SUT.

LEGEND:

SUT	System Under Test

(4) Port Enumeration. Port enumeration provides a list of services or applications running on the host and gives the tester a good indication of what operating system might be present on the end-point. When all the hosts in use by the SUT are determined, testers begin the initial evaluation of individual hosts. Each host is individually inspected for all available information, such as running services, operating system versions, and other applications. Information provided by investigating each device in-depth helps determine how susceptible an individual component of the SUT might be to a potential attack.

Enumeration, provided by port scanning of each host, provides a detailed list of which ports are open, closed, or filtered on a specified host. Port scans are conducted in a multitude of varieties using many different protocols, packet flags, and techniques. These various scans can yield different results in different situations, depending on the configurations and protections of each host.

Table E-11 shows the port enumeration test procedures, which use the following testing components: a laptop with a port scanning application installed, and assigned an IP address compliant with the test environment, and an Ethernet hub.

Table E-11. Port Enumeration Test Procedures

Procedure	Results
Available Hosts	During previous host discovery, the list of auditable components was defined and recorded.
Perform TCP/UDP Scan: A full TCP/UDP port scan will be completed on the known hosts in order to determine what services are available for further analysis. The following is an example of general TCP port scan of a list of know hosts: #NMAP –sS –n –P0 –p1- -iL test.ips.txt –oM 4amap.syn.txt –oA NMAP.syn.output.txt All ports, both TCP and UDP (65,535), should be scanned. (Note: There is a GUI available for the NMAP tool.)	The output of this scan will provide a list of open, closed, and filtered TCP ports for each host.
Perform UDP Scan: A full UDP scan will be completed to determine if there are any UDP services listening on the host. The following is an example of an UDP port scan regarding a list of known hosts: #NMAP –sU –p1- –host-timeout 300s –iL test.ips.txt –oM 4amap.udp.txt –oA NMAP.udp.output.txt	The output from this scan will provide a list of available UDP ports from the host list.
Operating System Enumeration: Another portion of detail that can be obtained during the port scan is the operating system. Generally during the Phase I process, the operating system is stated, but the ability to obtain the operating system type and version remotely can provide an attacker with added information. The following is an example of an operating system enumeration using xprobe: #xprobe –v –B –D 1 –D 2 192.168.1.100 NMAP can also be used to perform this function.	The results of this scan should reveal the operating system and version.
Additional Enumeration: At this point the tester may be satisfied with the data on available ports collected or may attempt to use other port scanning techniques suck as ACK scans, FIN scans, Null scans, or any other variety of techniques that might elicit a response from the host.	Not Applicable

LEGEND:

ACK	Acknowledge	TCP	Transfer Control Protocol
NMAP	Networked Messaging Application Protocol	GUI	Graphical User Interface
FIN	Finished	UDP	User Datagram Protocol

(5) Service Enumeration. Service enumeration determines what services are listening on an IP port of the SUT. Services and their versions can provide the tester with a list of known exploits or weakness that might be effective against a given target. Service enumeration takes many forms. Banner grabbing, which is another form of service enumeration, uses a specified application to match a service response to a known repository of responses. Those responses are then used to determine the service and its version. Banner grabbing might be as easy as using Telnet to connect to a port or opening a web browser to view a web-based application. Table E-12 shows the service enumeration test procedures using the list of open TCP ports as components.

Table E-12. Service Enumeration Test Procedures

Procedure	Results
Evaluate Open Ports: Evaluate the open ports to determine what services are listening on each of the available ports. There are a number of applications that provide this function. The following is an example of a general service enumeration of a known list of hosts and ports: #amap –A –v –i 4amap.syn.txt another option would be: #NMAP –sV –p portlist.txt –iL test.ips.txt It is recommended that all TCP/UDP ports be scanned. (–p1-65535)	All ports that have services bound will be enumerated. Common services include those that can be found bound to TCP ports 1-1024. Custom services may be found on ports above 1024.
LEGEND: NMAP Networked Messaging Application Protocol TCP Transfer Control Protocol	UDP User Datagram Protocol

(6) Service Analysis. Service analysis provides the test team with specific service details that could be used in attacking the system. When a service is known, a variety of checks may be completed against it. The list of possible checks is as large as the number of services that could run on a host. Examples include permission settings, authentication requirements, or information disclosure. Each of these checks is specific to the service. Table E-13 shows the service analysis test procedures using the list of available services as components.

Table E-13. Service Analysis Test Procedures

Procedure	Results
Service Analysis: 1. Upon determining the services available to be tested, the tester can perform services analysis. 2. Service analysis is wide ranging and the tools and techniques used are based on the services present. 3. The following is an example analysis of the Secure Shell (SSH) service running on a remote host. The telnet command provides a banner that identifies the service version, which can be compared to current versions and vulnerabilities. The second command attempts to authenticate with SSH v1, which is inherently weaker than Version 2: >telnet 192.168.1.100 22 SSH-1.99-OpenSSH_3.9p1 #ssh –1 192.168.100 The number of checks for service analysis is nearly limitless.	The Internet Protocol (IP) vulnerability tester will analyze the results of the discovered services and determine if there are vulnerabilities associated with the service.
LEGEND: IP Internet Protocol	SSH Secure Shell

c. Vulnerability Assessment. Vulnerability assessment provides an automated process to determine if a system or application is vulnerable to attack. Vulnerability assessment tools provide the test team an automated process for taking the system and service enumeration information and matching it to known attacks. An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack. Performing a vulnerability assessment manually, on a large scale, is time consuming; automated applications provide this information more efficiently. Although modern vulnerability scanners are accurate, a vulnerability scanner’s results are always analyzed by the test team to eliminate false positives and to ensure additional findings are not overlooked.

(1) Vulnerability Scan. A vulnerability scan checks remote targets for possible vulnerabilities. This automated process generally detects vulnerabilities on the host operating system and on many of the common applications that run on the host’s operating systems. Some examples of common applications that are checked by a vulnerability scan are web services, mail applications, file transfer applications, and remote access applications such as telnet or Secure Shell. Vulnerability scans take the response-and-discovery information they receive during a scan and match this information to a list of known attacks and exploits to determine what possible attacks could be executed against each host. Vulnerability scanners detect information from a remote target in various ways. Some scanners require local login credentials while others rely on services such as remote registry. Some rely solely on banner grabbing and port scans. Table E-14 shows the vulnerability assessment test procedures, which use open ports as input.

Table E-14. Vulnerability Assessment Test Procedures

Procedure	Results
1. The testing platform is connected to a port that is shared by the product under evaluation, much like the host discovery portion of the test. 2. Using the data collected from the host discovery and device investigation portion of the testing, the system configures a vulnerability scan with a vulnerability assessment application. 3. The configuration of the tool is set to one of several options depending on the test team’s earlier discoveries. 4. The vulnerability scanner is configured to enable all checks, even the checks that could be considered harmful or cause denial of service. The tester then provides the known hosts and selects the known open ports on the target host and executes the assessment. 5. This procedure could be used with more than one vulnerability scanner and may require that user credentials be provided for the hosts depending on results desired from the test team.	The test team should evaluate the output of the scans to determine if the audit produced any false positives. The output of multiple vulnerability assessments is compared for like results and any variances. Any true positives should be further analyzed and documented. This information will be used during the exploitation and penetration testing phase.

d. User Application Assessment. The user application assessment provides detailed information about the host and its applications. The interface provides access to the system or access to data on the system. User interfaces, although convenient for users, can provide an attacker with a wealth of information about the remote host. Many techniques and tools are available for attempts to attack an application. An example of possible attack on a user interface is a web attack that uses sequential or non-random session keys for users. This type of attack can allow an attacker to reuse session keys or possibly cookies to access a site as an authorized user. Other times, interfaces do not protect the data they are sending and, while in transit, that information can be seen in the clear utilizing a network sniffer device.

(1) Application Assessment. The vulnerability assessment of an individual application is much like a general vulnerability assessment. However, in this case, the scan is against a specific type of application such as a web server or database application. Application vulnerability scanners use specific attacks associated with the types of applications they are designed to attack. Some very common application assessment tools include web services and database applications. Applications can be even more specialized for a specific type of web service or database, such as Microsoft Internet Information Service or an Oracle database. These tools look for specific vulnerabilities within their given applications. Unlike a network or system vulnerability scanner, application assessment tools know about a single application and nothing about other applications, except as they explicitly relate to the application within the scope of the tool. Additional testing procedures are available in Appendices A and B of this document. Table E-15 shows the application assessment test procedures using the following components:

- Web server IP
- Web application authentication information
- Web application vulnerability scanner

Table E-15. Application Assessment Test Procedures

Procedure	Results
The first step in application assessment would be to define the web applications that are present on the hosts. The service enumeration portion of the test provides this information. For each service listed, an application assessment tool is selected to perform a security evaluation. The following command is executed using the web assessment tool Nikto to evaluate a singe host's web services on a given host: #perl nikto.pl –C all –port 80 –host 192.168.1.100 The following attempts to evaluate an Server Message Block administrator login with a list of passwords in a text file: #medusa –h 192.168.1.100 –u administrator –P passwords.txt –e ns –M smbnt As mentioned above, these are just examples of possible scenarios that the test team might attempt.	The test team should evaluate the output of the scans to determine if the audit produced any false positives.

e. Denial of Service (DoS). Attempting a DoS attack determines the SUT's susceptibility to actions such as malformed packets or port message flooding. The testing team might take a particular end-point offline to capture one of its attributes, such as an IP address or a Media Access Control address. By knocking a node offline, the test team may be able to impersonate a device or receive traffic that was not intended for them. Another approach to a DoS attack is generating customized packets or streams of packets to be sent to a remote host. Some packets, such as fragmented, un-sequential, or unacknowledged, may cause the network stack or some other functionality of the system to halt, thus creating a DoS attack against the system.

The specific procedure used for DoS testing varies and is generally dependent on both the SUT and the toolset used to exploit it. The following test procedures are meant to serve only as representative examples of DoS attacks and are not intended to describe a comprehensive procedure for all types of DoS attacks. Table E-16 shows the DoS test procedures using the components listed below:

- A list of ports, protocols, and services identified as active on the SUT

- Known exploits (in the form of tools or scripts) against specific enumerated protocols and services

Table E-16. DoS Test Procedures

Procedure	Results
1. Search out and download exploits for various known vulnerabilities that affect major system resources, protocols, applications, and services. A variety of sources exist that contain scripts, tools, and procedures for exploiting known vulnerabilities that cause DoS in a variety of applications and operating systems. Examples of sources include insecure.org's "Exploit World" (<http://www.insecure.org/sploits.html>) and SecurityFocus (<http://www.securityfocus.com/tools> and <http://www.securityfocus.com/pen-test>). 2. Obtain a list of all active IP addresses and active ports and services on the SUT. 3. Using available exploit tools and scripts, set up a DoS attack against one or more of the SUT's active applications or services. An example of a DoS attack includes the following: SYN Flood Attack: Consists of sending one or more of the SUT's components a series of TCP SYN requests from a spoofed IP address, the goal being to overwhelm the target system with unanswered requests, thus causing the system to crash. Phreeon's BlitzNet script (available from <http://www.megasecurity.org>/DoS/blitznet.html) enables testers to conduct a SYN Flood Attack against a remote server from one or more computers without logging onto any of them. 4. Launch the DoS program against the remote host to be tested.	Depending upon whether or not the SUT has been correctly configured, the system resources of the component under attack will either become overwhelmed (leading to a system lock-up or crash) or will drop the fragmented packets and continue to operate with little or no impact on system resources. The Core Impact tool is recommended for automating this test.

LEGEND:

DoS	Denial of Service	SYN	Synchronize
IP	Internet Protocol	TCP	Transmission Control Protocol
SUT	System Under Test		

f. Exploitation. An Exploitation attempts to use known flaws that have been exploited in existing applications, operating systems, and services. Exploitation is used not only to categorically verify that the vulnerability exists (and is not a false-positive), but also to gain visibility and access to hosts or data not initially accessible. Compromising the host can be as simple as accessing an account that uses a default or null password, or as complicated as creating a custom exploit script to exploit vulnerabilities in a software application. The list of techniques available to take control of a host is endless, with new and unique attacks being created daily.

The general procedure is determined, in part, by the results of enumeration and information gathering that was performed previously. The test team examines the list of known vulnerabilities and potential security holes on all of the target hosts and determines which are most likely to be targeted for exploitation. Next, the team will attempt to exploit those vulnerabilities to gain illegal access to the target system.

(1) Exploit Code. An exploit script is necessary to verify that vulnerabilities exist, or to compromise the remote host. Using an exploit script can have negative effects on remote hosts and is generally not used freely outside of a lab or testing environment. An exploit script can be gathered from public channels on the Internet or created in-house by the testing team.

(a) Injection. There are many different types of injection techniques and tools. One of the most common injection techniques is attempting Structured Query Language

(SQL) injection through web interfaces that are supported by SQL back ends. During previous network and application analysis, the test team would discover and analyze vulnerabilities in application and network injection and, based on this data, would attempt to compromise the remote host. Table E-17 shows the exploitation and injection test procedures using the components listed below.

- List of possible vulnerable services found in previous tests
- Access to exploit code and/or procedures

Table E-17. Exploitation and Injection Test Procedures

Procedure	Results
1. Search out and download exploits for the various known vulnerabilities that may affect the services that were previously found to be vulnerable. A variety of sources exist that contain scripts, tools, and procedures for exploiting known vulnerabilities that may cause security violations in a variety of applications and operating systems. Examples of sources include insecure.org's "Exploit World" (<http://www.insecure.org/sploits.html> and SecurityFocus (<http://www.securityfocus.com/tools> and <http://www.securityfocus.com/pen-test>). 2. Obtain a list of all active IP addresses and active ports and services on the SUT. Version numbers of the services found should be recorded. 3. Using available exploit tools and scripts, attempt to exploit the vulnerability on the affected component of the SUT. Depending on the type of vulnerability, exploitation may consist of running a generally available script, creating a new script, or manipulating a web based application in a fashion not intended during normal functioning of the SUT. There are many services that IP ports could be bound to. This test plan does not attempt to detail plans and procedures for each one. However, services like SQL, SSH, LDAP, and SNMP are just a few of the more popular services used on the equipment within the DSN. 4. Launch the exploit against the service to be tested.	Depending on the type of vulnerability, the following actions may occur: 1. The tester may gain control of the system. 2. The system may become unresponsive. 3. The tester may obtain information from the SUT that would not normally be revealed. The Metasploit and Core Impact tools are recommended for automating this test.

LEGEND:

DSN	Defense Switched Network	SQL	Structured Query Language
IP	Internet Protocol	SSH	Secure Shell
LDAP	Lightweight Directory Access Protocol	SUT	System Under Test
SNMP	Simple Network Management Protocol		

g. Password Cracking. Password testing determines if a password's strength is sufficient, given the type of hashing or encryption used to protect the system. Testing or cracking encrypted or hashed passwords can be time consuming, depending on the source of the passwords. The test team uses several methods to test passwords. Many common user passwords can be determined by dictionary attacks using common password validation tools such as *l0phtcrack* or *John the Ripper*. In situations where dictionary attacks are not sufficient, brute force and hybrid (brute force and dictionary) attacks may discover the password. Another technique is to compare the password hash to a known list of password hashes for a match. This list is commonly referred to as a rainbow table. Table E-18 shows the password cracking test procedures, which use the password file and hash components.

Table E-18. Password Cracking Test Procedures

Procedure	Results
1. Obtain the password file or password hashes from the host in question. This might require the password file on a windows box, the shadow file on a Linux machine, or a configuration file from a network element. 2. The procedure for obtaining these files may vary. The file may be provided by the vendor or copied after the host is compromised. 3. Evaluate the password file using an appropriate password cracking tool. The following command is an example of using *John the Ripper* to attempt a standard dictionary attack on a Linux shadow file: ./john –show –wordfile:dictionary.txt host.shadow For Session Initiation Protocol password cracking, tools such as svcrack or SIPtastic can be used.	The results may be a discovered password that is easily cracked. The absence of any results will indicate that a strong password policy is in effect.

8. Institute for Security and Open Methodologies Open Source Security Testing Methodology Manual Procedures for Systems Service Identification.

Testers may use the following Open Source Security Testing Methodology Manual (OSSTMM) strategies.

a. Expected Results:

- Open, closed, or filtered ports.
- IP addresses of live systems.
- Internal system network addressing.
- List of discovered tunneled and encapsulated protocols.
- List of discovered routing protocols supported.
- Active services.
- Service types.
- Service application type and patch level.
- Operating System type.
- Patch level.
- System type.
- List of live systems.
- Internal system network addressing.
- Network map.

b. Enumerate Systems:

- Collect broadcast responses from the network.
- Probe past the firewall with strategically set packet Time to live settings (Firewalking) for all (IP) addresses.
- Use ICMP and reverse name lookups to determine the existence of all the machines in a network.
- Use a TCP source port 80 and acknowledge on ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000 for all hosts in the network.

- Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use a TCP SYN on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use Domain Name Server connect attempts on all hosts in the network.
- Use File Transfer Protocol and Proxies to bounce scans to the inside of the Demilitarized Zone for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

c. Enumerating Ports:

- Use TCP SYN (Half-Open) scans to enumerate ports as being open, closed, or filtered on the default TCP testing ports for all the hosts in the network.
- Use TCP full connect scans to scan all ports up to 65,535 on all hosts in the network.
- Use TCP fragments in reverse order to enumerate ports and services for the subset of ports on the default packet fragment testing ports in Appendix B for all hosts in the network.
- Use User Datagram Protocol (UDP) scans to enumerate ports as being open or closed on the default UDP testing ports if UDP is **not** being filtered already. [Recommended: first test the packet filtering with a small subset of UDP ports.]

d. Verifying Various Protocol Response:

- Verify and examine the use of traffic and routing protocols.
- Verify and examine the use of non-standard protocols.
- Verify and examine the use of encrypted protocols.
- Verify and examine the use of TCP and ICMP over IP version 6.

e. Verifying Pack Level Response:

- Identify TCP sequence predictability.
- Identify TCP initial sequence numbers predictability.
- Identify IP identification sequence generation predictability.
- Identify system up-time.

f. Identifying Services:

- Match each open port to a service and protocol.
- Identify server uptime to latest patch releases.
- Identify the application behind the service and the patch level using banners or fingerprinting.
- Verify the application to the system and the version.
- Locate and identify service remapping or system redirects.
- Identify the components of the listening service.

- Use UDP-based service and trojan requests to all the systems in the network.

g. Identifying Systems:

- Examine system responses to determine operating system type and patch level.
- Examine application responses to determine operating system type and patch level.
- Verify the TCP sequence number prediction for each live host on the network.
- Match information gathered to system responses for more accurate results.

9. Institute for Security and Open Methodologies Open Source Security Testing Methodology Manual Procedures for Internet Application Testing. Testers may use the following OSSTMM strategies.

a. Expected Results:

- Applications.
- Application components.
- Application vulnerabilities.
- Application system trusts.

b. Re-Engineering:

- Decompose or deconstruct the binary codes, if accessible.
- Determine the protocol specification of the server/client application.
- Determine program logic from the error/debug messages in the application output and program behavior/performance.

c. Authentication:

- Find possible brute force access points in the applications.
- Attempt a valid login credential with password grinding.
- Bypass authentication system with spoofed tokens.
- Bypass authentication system with replay authentication information.
- Determine the application logic to maintain the authentication session—number of (consecutive) failure logins allowed, login timeout, etc.
- Determine the limitations of access control in the applications—access permissions, login session duration, idle duration.

d. Session Management:

- Determine the session management information—number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, session Identification (ID) in Uniform Resource

Locater (URL) encoding string, session ID in hidden HyperText Markup Language (HTML) field variables, etc.

- Guess the session ID sequence and format.
- Determine the session ID is maintained with IP address information. Verify if the same session information can be retried and reused in another machine.
- Determine the session management limitations—bandwidth usages, file download/upload limitations, transaction limitations, etc.
- Gather excessive information with direct URL, direct instruction, action sequence jumping, and/or page skipping.
- Gather sensitive information with Man-In-the-Middle attacks.
- Inject excess/bogus information with session-hijacking techniques.
- Replay gathered information to fool the applications.

e. Input Manipulation:

- Find the limitations of the defined variables and protocol payload—data length, data type, construct format, etc.
- Use exceptionally long character-strings to find buffer overflow vulnerabilities in the applications.
- Concatenate commands in the input strings of the applications.
- Inject Structured Query Language in the input strings of database-tired web applications.
- Examine "cross-site scripting" in the web applications of the system.
- Examine unauthorized directory/file access with path/directory traversal in the input strings of the applications.
- Use specific URL-encoded strings and/or unicode-encoded strings to bypass input validation mechanisms of the applications.
- Execute remote commands through "server side include."
- Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.
- Manipulate the hidden field variable in the HTML forms to fool or modify the logic in the server-side web applications.
- Manipulate the "referrer," "host," etc., HyperText Transfer Protocol variables to fool or modify the logic in the server-side web applications.
- Use illogical input to test the application error-handling routines and to find useful debug/error messages from the applications.

f. Output Manipulation:

- Retrieve valuable information stored in the cookies.
- Retrieve valuable information from the client application cache.
- Retrieve valuable information stored in the serialized objects.
- Retrieve valuable information stored in the temporary files and objects.

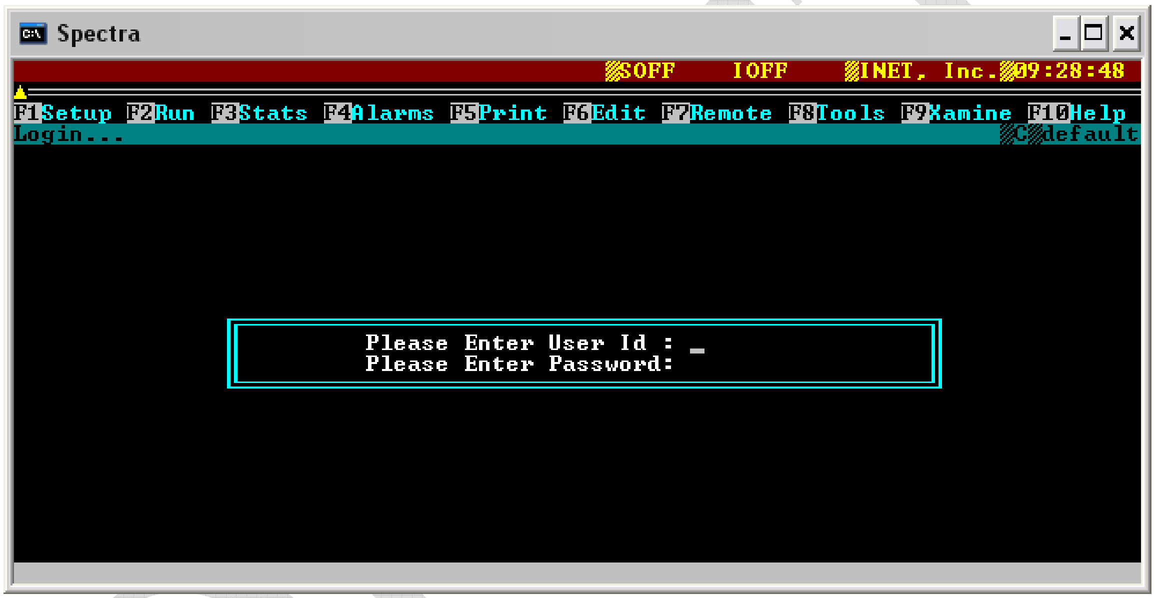
g. Information Leakage:

- Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.
- Examine the information contained in the application banners, usage instructions, welcome messages, farewell messages, application help messages, debug/error messages, etc.

10. Spectra Training Guide for SS7 and ISDN Protocols.

a. Logon to Spectra

(1) Click on Spectra icon on the desktop of the laptop.
(2) Press any key.
(3) Enter user ID and password. See Figure E-6.


Spectra
SOFF IOFF INET, Inc. 09:28:48
F1Setup F2Run F3Stats F4Alarms F5Print F6Edit F7Remote F8Tools F9Xamine F10Help
C default

```
Login...

Please Enter User Id : _
Please Enter Password:
```

Figure E-6. Logon Screen

b. Design Layout of Spectra

(1) Running Mode indicated in the top red bar, as shown in Figure E-7.
(a) SOFF = Signaling System 7 (SS7).
(b) IOFF = Integrated Services Digital Network (ISDN).

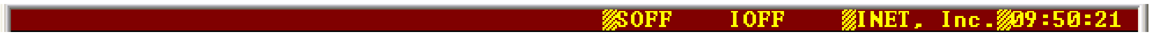
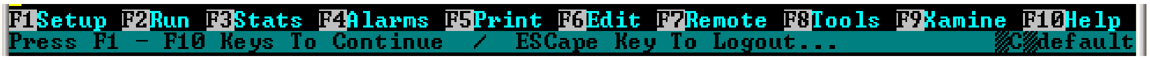


Figure E-7. Running Mode

(2) All function keys are shown in the top border line, as shown in Figure E-8.



```
F1Setup F2Run F3Stats F4Alarms F5Print F6Edit F7Remote F8Tools F9Xamine F10Help
Press F1 - F10 Keys To Continue  /  ESCape Key To Logout...              ▨C▨default
```

Figure E-8. Function Keys

(3) Capture buffer indicator is a double white line that shows blue when buffer is full, as shown in Figure E-9.

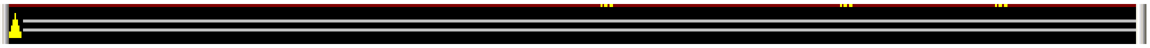


Figure E-9. Capture Buffer Indicator

(4) Yellow triangle is the capture pointer and indicates the capacity of the Random Access Memory (RAM). When the capacity is maxed, the capture will stop. See Figure E-19.

(5) Bottom border line shows the Links "In Service" or "Out of Service."

c. Spectra Function Keys

(1) Key – F1 – Setup. See Figure E-10.

(a) Configure Level 1 physical interface properties for T1 and E1.

(b) Configure Level 2 SS7 or Integrated Services Digital Network (ISDN) protocols.

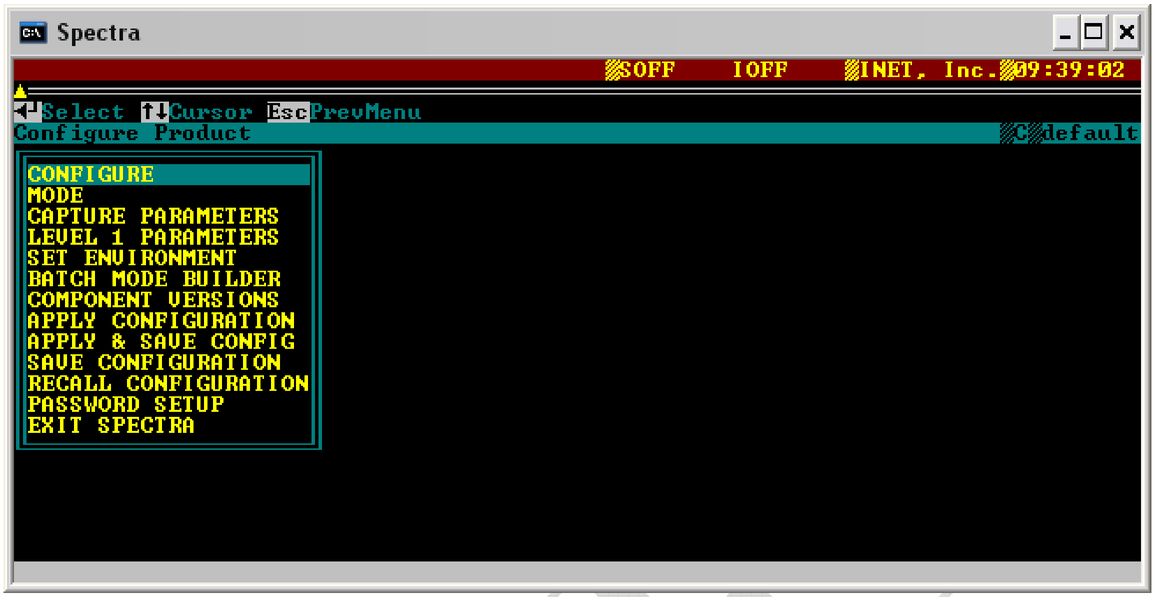
(c) Configure Level 3 SS7 network point codes, links and Link Sets (LS).

(d) ISDN Service Access Point Identifier (SAPIs), Terminal Equipment Identifier (TEIs) and protocols.

(e) Configure filters.

(f) Configure auto responses.

(g) Save and recall configurations.



```
Spectra
                                          ▒SOFF     IOFF     ▒INET, Inc.▒09:39:02
↵Select ↑↓Cursor EscPrevMenu
Configure Product                                                       ▒C▒default
 CONFIGURE
 MODE
 CAPTURE PARAMETERS
 LEVEL 1 PARAMETERS
 SET ENVIRONMENT
 BATCH MODE BUILDER
 COMPONENT VERSIONS
 APPLY CONFIGURATION
 APPLY & SAVE CONFIG
 SAVE CONFIGURATION
 RECALL CONFIGURATION
 PASSWORD SETUP
 EXIT SPECTRA
```

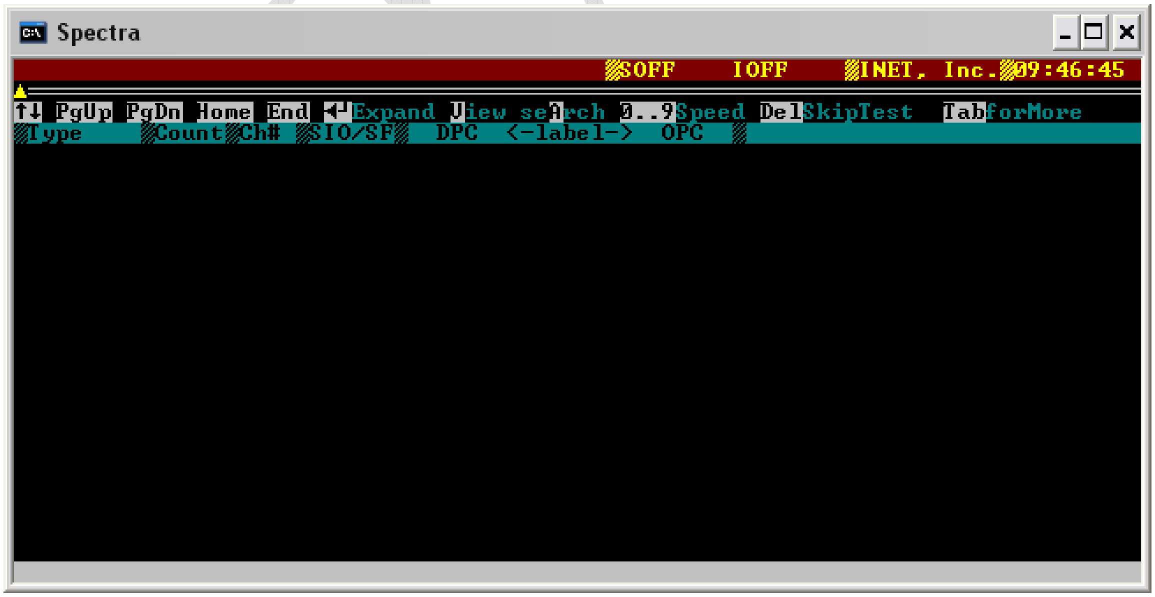
Figure E-10. F1 Setup

(2) Key – F2 – Run/Capture. See Figure E-11.

(a) Capture buffer view. Data is displayed for post-filtering to include tagging and marking.

(b) Real-time signaling messages displayed.

(c) Grab function available for storing messages to the message editor (F6).



```
Spectra
                                          ▒SOFF     IOFF     ▒INET, Inc.▒09:46:45
↑↓ PgUp PgDn Home End ↵Expand View seArch 0..9Speed DelSkipTest  TabforMore
▒Type     ▒Count▒Ch#  ▒SIO/SF▒  DPC  <-label->  OPC  ▒
```

Figure E-11. F2 Run/Capture

(3) Key – F3 – Statistics. See Figure E-12.

(a) Basic statistics for SS7 and ISDN.

1. Level 1 – T1/E1 Signal, Sync AIS.

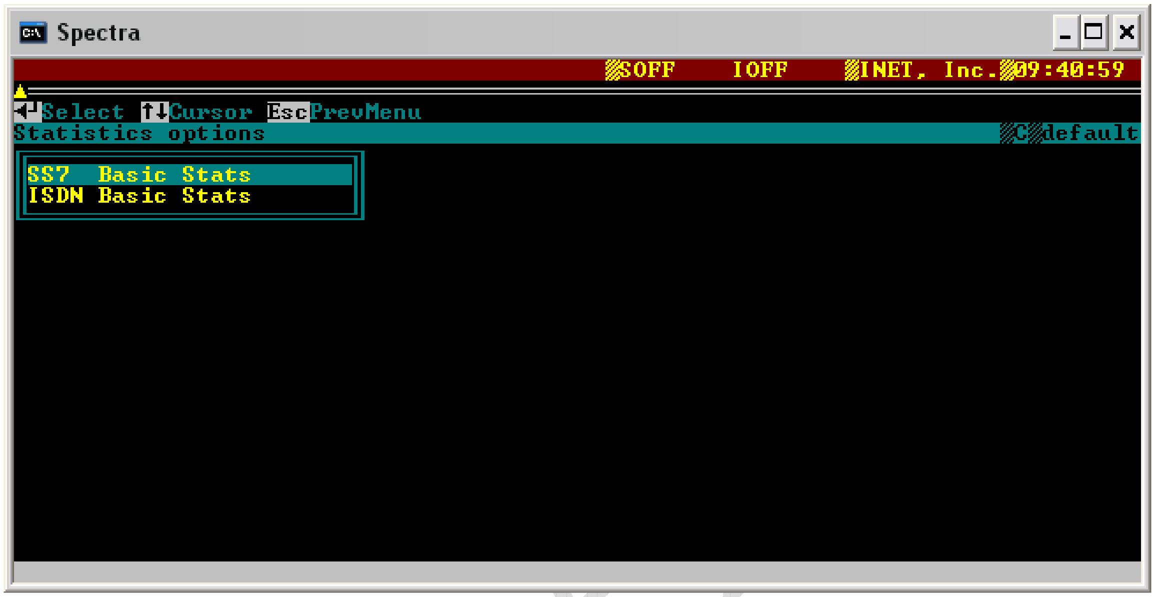
2. Level 2 – Link Status Signal Unit, Message Signal Unit, Receive Ready and Unnumbered Acknowledgment.

3. Level 3 – SS7 Signaling Network Management message count.

4. Level 4 – SS7 and ISDN message counts.

5. ISDN User Part (ISUP) call statistics.

6. ISDN call generator statistics.



```
Spectra
                                                  ▒SOFF      IOFF     ▒INET, Inc.▒09:40:59
↵Select ↑↓Cursor EscPrevMenu
Statistics options                                                                ▒C▒default
 SS7  Basic Stats
 ISDN Basic Stats
```

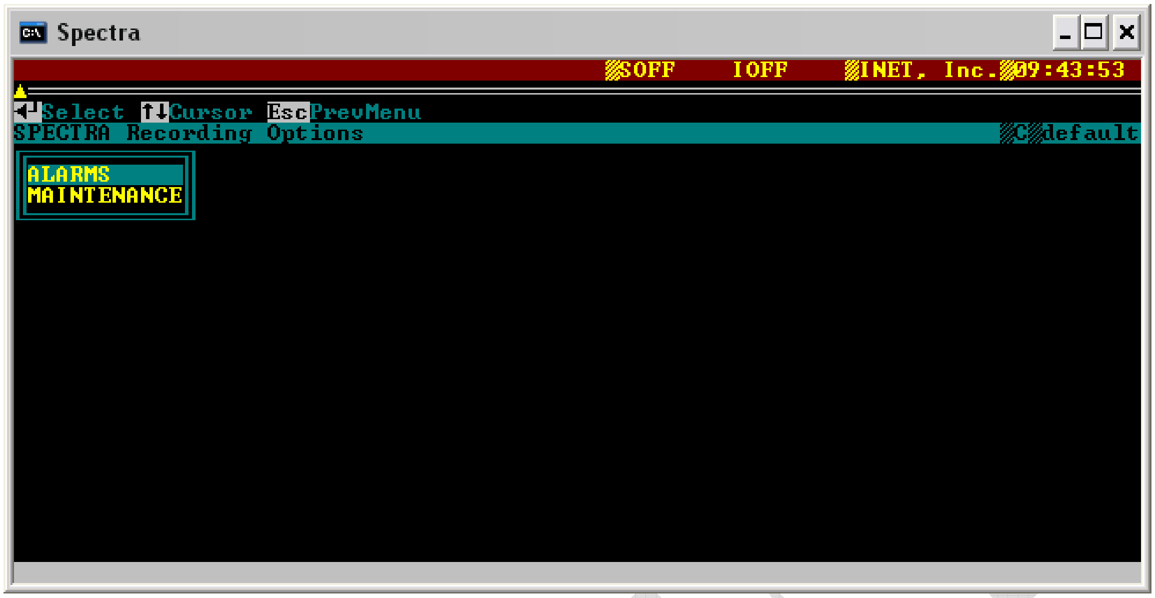
Figure E-12. F3 Statistics

(4) Key – F4 – Alarms. See Figure E-13.

(a) System integrity alarms.

(b) Links status.

(c) Event logs.



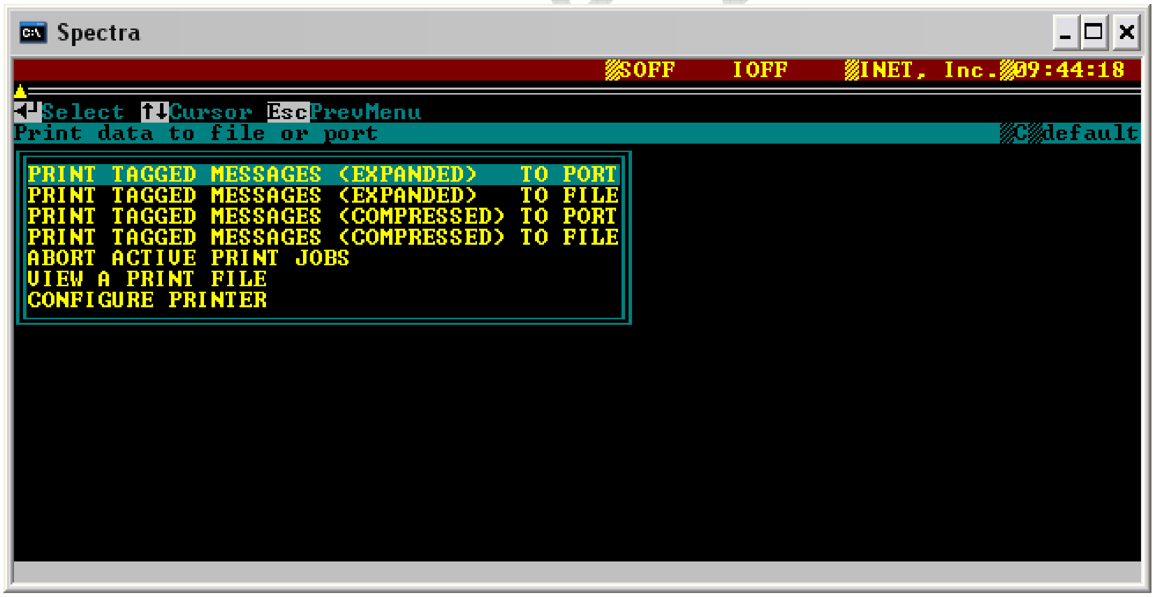
```
Spectra
                                                          ▒SOFF    IOFF    ▒INET, Inc.▒09:43:53
↵Select ↑↓Cursor EscPrevMenu
SPECTRA Recording Options                                                          ▒C▒default
 ALARMS
 MAINTENANCE
```

Figure E-13. F4 Alarms

(5) Key – F5 – Print. See Figure E-14.

(a) Print in compressed or expanded format.

(b) “Marked” or “Tagged” (F2 or F9) data can be converted into American Standard Code for Information Interchange (ASCII) messages.



```
Spectra
                                                          ▒SOFF    IOFF    ▒INET, Inc.▒09:44:18
↵Select ↑↓Cursor EscPrevMenu
Print data to file or port                                                         ▒C▒default
 PRINT TAGGED MESSAGES (EXPANDED)   TO PORT
 PRINT TAGGED MESSAGES (EXPANDED)   TO FILE
 PRINT TAGGED MESSAGES (COMPRESSED) TO PORT
 PRINT TAGGED MESSAGES (COMPRESSED) TO FILE
 ABORT ACTIVE PRINT JOBS
 VIEW A PRINT FILE
 CONFIGURE PRINTER
```

Figure E-14. F5 Print

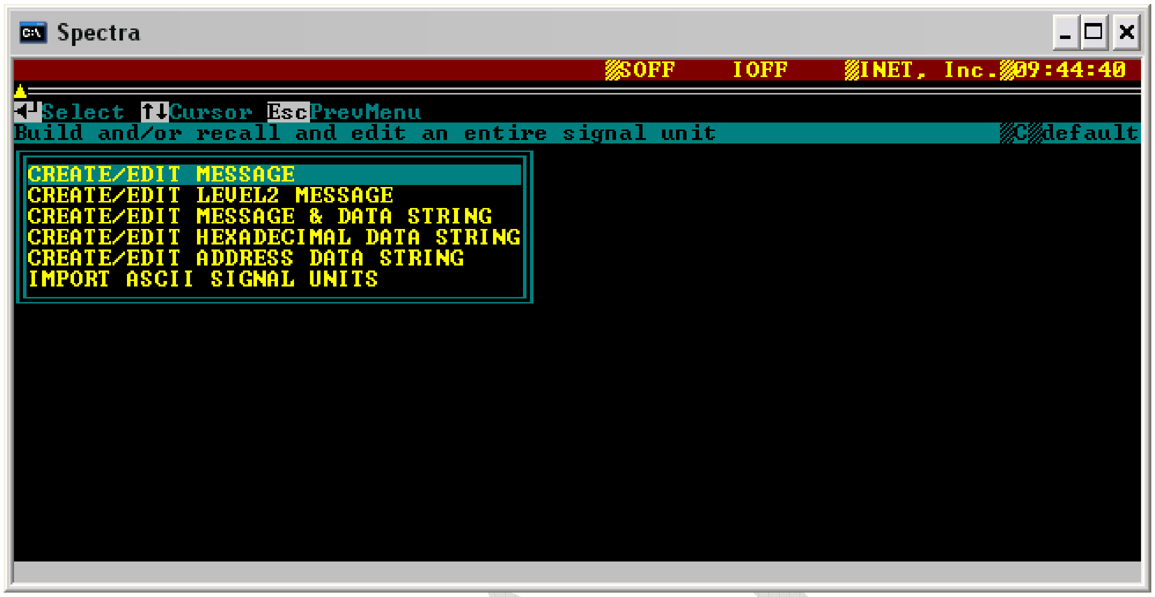
(6) Key – F6 – Editor. See Figure E-15.

(a) Recall messages for editing.

(b) Save messages for use in a call script.

(c) Add optional parameters to ISUP messages.

(d) Add additional Information Elements (IE) to ISDN messages.
(e) Send message to F5 print with a "*".
(f) End "E" to truncate the message.



Spectra
▒SOFF IOFF ▒INET, Inc.▒09:44:40
↵Select ↑↓Cursor EscPrevMenu
▒C▒default
CREATE/EDIT MESSAGE
CREATE/EDIT LEVEL2 MESSAGE
CREATE/EDIT MESSAGE & DATA STRING
CREATE/EDIT HEXADECIMAL DATA STRING
CREATE/EDIT ADDRESS DATA STRING
IMPORT ASCII SIGNAL UNITS

```
Build and/or recall and edit an entire signal unit
```

Figure E-15. F6 Editor

(7) Key – F7 – Remote.
NO LONGER IN USE.

(8) Key – F8 – Tools. See Figure E-16.
(a) DOS command directory.
(b) Sending message out "on demand."
(c) Taking SS7 or ISDN links "out of service."
(d) Connecting or disconnecting SS7 Virtual Signaling Point (VSP).

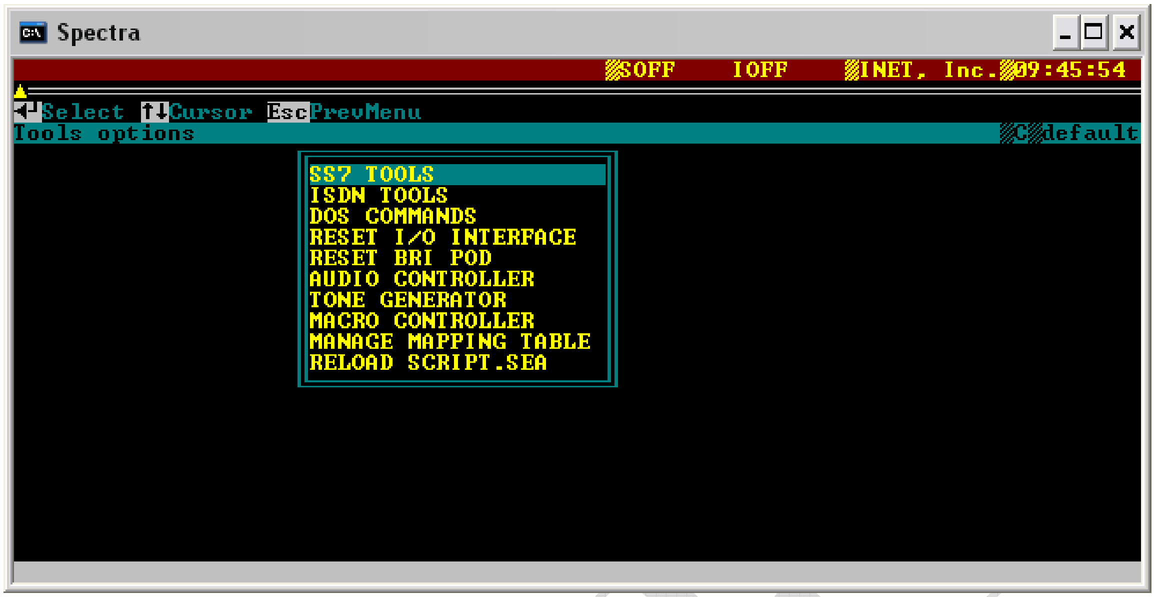


Figure E-16. F8 Tools

(9) Key – F9 – Examine. See Figure E-17.

(a) This is the stop key. It stops all call generators and message capturing when pressed.

(b) "S" save the capture.

(c) "R" recall the capture.

(d) "G" grab and store the message.

(e) "K" mark the message for print.

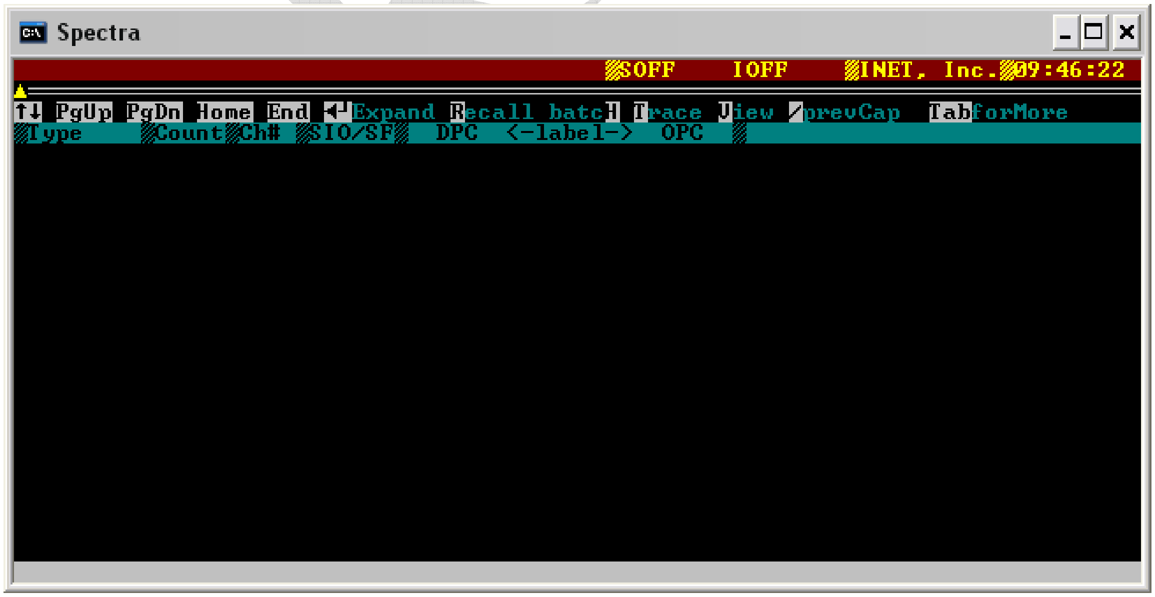
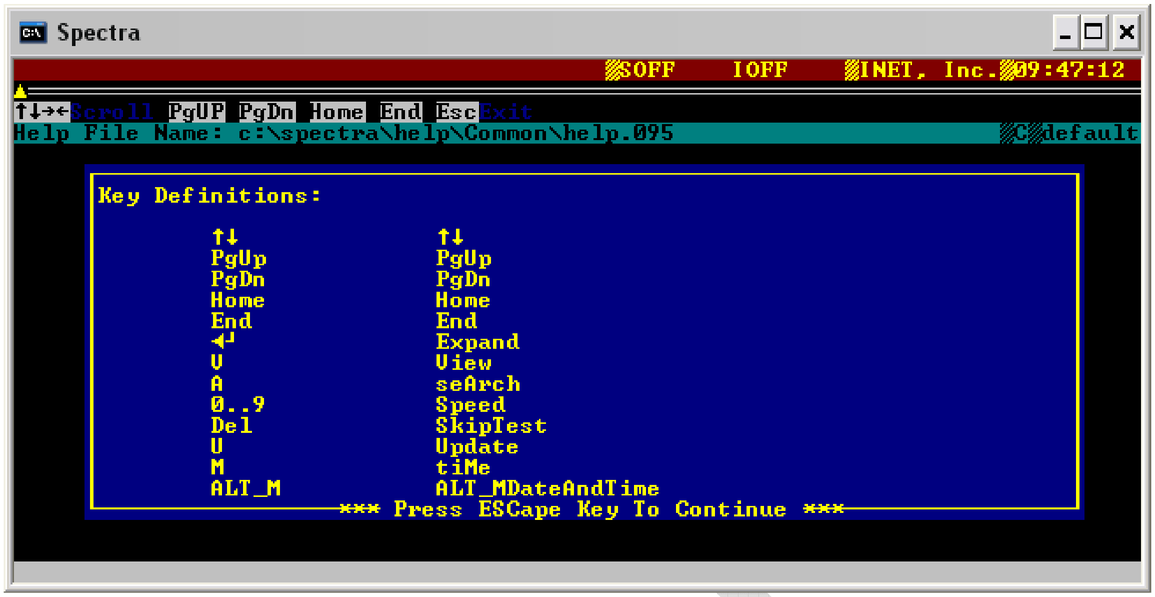

Spectra
SOFF IOFF INET, Inc. 09:46:22
↑↓ PgUp PgDn Home End Expand Recall batcH Trace View /prevCap TabforMore
Type Count Ch# SIO/SF DPC <-label-> OPC

Figure E-17. F9 Examine

(10) Key – F10 – Help. See Figure E-18.

(a) Spectra help guide.



```
Spectra
                                              SOFF    IOFF    INET, Inc. 09:47:12
↑↓→←Scroll PgUP PgDn Home End Esc Exit
Help File Name: c:\spectra\help\Common\help.095                         C default

      Key Definitions:

                ↑↓               ↑↓
                PgUp             PgUp
                PgDn             PgDn
                Home             Home
                End              End
                ↵                Expand
                V                View
                A                seArch
                0..9             Speed
                Del              SkipTest
                U                Update
                M                tiMe
                ALT_M            ALT_MDateAndTime
                     *** Press ESCape Key To Continue ***
```

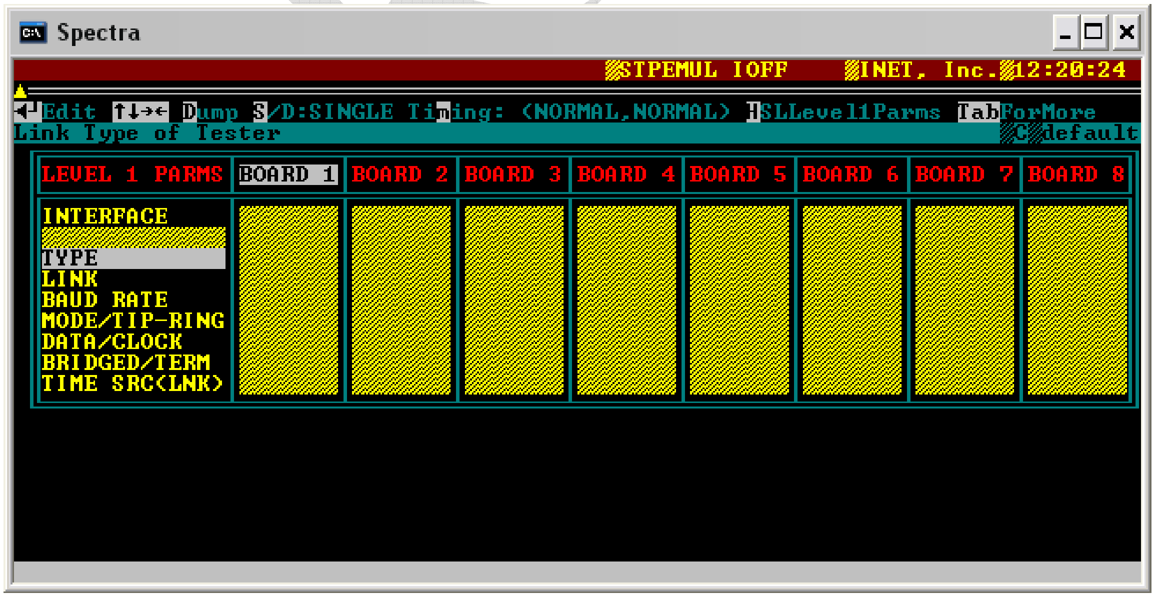
Figure E-18. F10 Help

d. Configuring an SS7 Network

(1) Reference: Real Time Services Information Assurance Test Plan, Section E-7.2, RTS TDM Protocol Security Analysis Table E-14, Test Cases 1-30.

(2) Configure Level 1. See Figure E-19.

(a) Instructions: F1 → Level 1 Parameters → press enter.

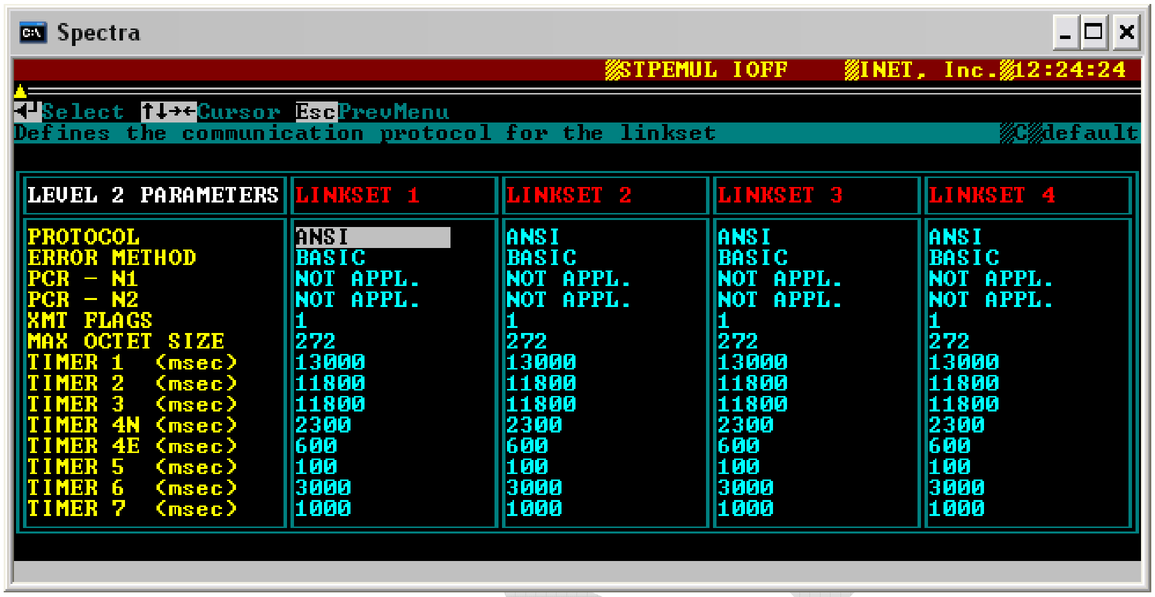


```
Spectra
                                              STPEMUL IOFF    INET, Inc. 12:20:24
↵Edit ↑↓→← Dump S/D:SINGLE Timing: (NORMAL,NORMAL) HSLLevel1Parms TabForMore
Link Type of Tester                                                     C default

 LEVEL 1 PARMS | BOARD 1 | BOARD 2 | BOARD 3 | BOARD 4 | BOARD 5 | BOARD 6 | BOARD 7 | BOARD 8

 INTERFACE
 TYPE
 LINK
 BAUD RATE
 MODE/TIP-RING
 DATA/CLOCK
 BRIDGED/TERM
 TIME SRC(LNK)
```

Figure E-19. Configuration Level 1

(3) Configure Level 2 – American National Standards Institute (ANSI) or International Telecommunications Union – Most common protocol is ANSI. See Figure E-20.

(a) Instructions: F1 → Configure → SS7 → Level 2 Parameters.



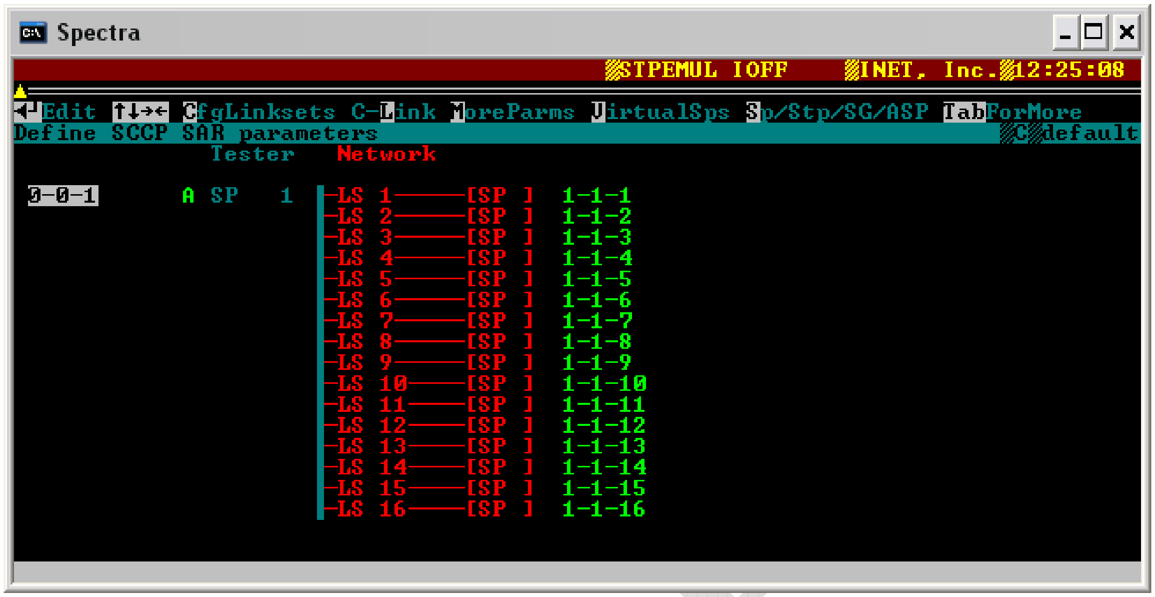
```
                                        ▒STPEMUL IOFF    ▒INET, Inc.▒12:24:24
↵Select ↑↓→←Cursor EscPrevMenu
Defines the communication protocol for the linkset                  ▒C▒default

 LEVEL 2 PARAMETERS  LINKSET 1    LINKSET 2    LINKSET 3    LINKSET 4

 PROTOCOL            ANSI         ANSI         ANSI         ANSI
 ERROR METHOD        BASIC        BASIC        BASIC        BASIC
 PCR - N1            NOT APPL.    NOT APPL.    NOT APPL.    NOT APPL.
 PCR - N2            NOT APPL.    NOT APPL.    NOT APPL.    NOT APPL.
 XMT FLAGS           1            1            1            1
 MAX OCTET SIZE      272          272          272          272
 TIMER 1  (msec)     13000        13000        13000        13000
 TIMER 2  (msec)     11800        11800        11800        11800
 TIMER 3  (msec)     11800        11800        11800        11800
 TIMER 4N (msec)     2300         2300         2300         2300
 TIMER 4E (msec)     600          600          600          600
 TIMER 5  (msec)     100          100          100          100
 TIMER 6  (msec)     3000         3000         3000         3000
 TIMER 7  (msec)     1000         1000         1000         1000
```

Figure E-20. Configuration Level 2

(4) Configure Level 3 – Define signaling links (boards) with the Signaling Link Code (SLC) values. See Figure E-21.

(a) Instructions: F1 → Configure → SS7 → Level 3 Parameters → Network Configuration.

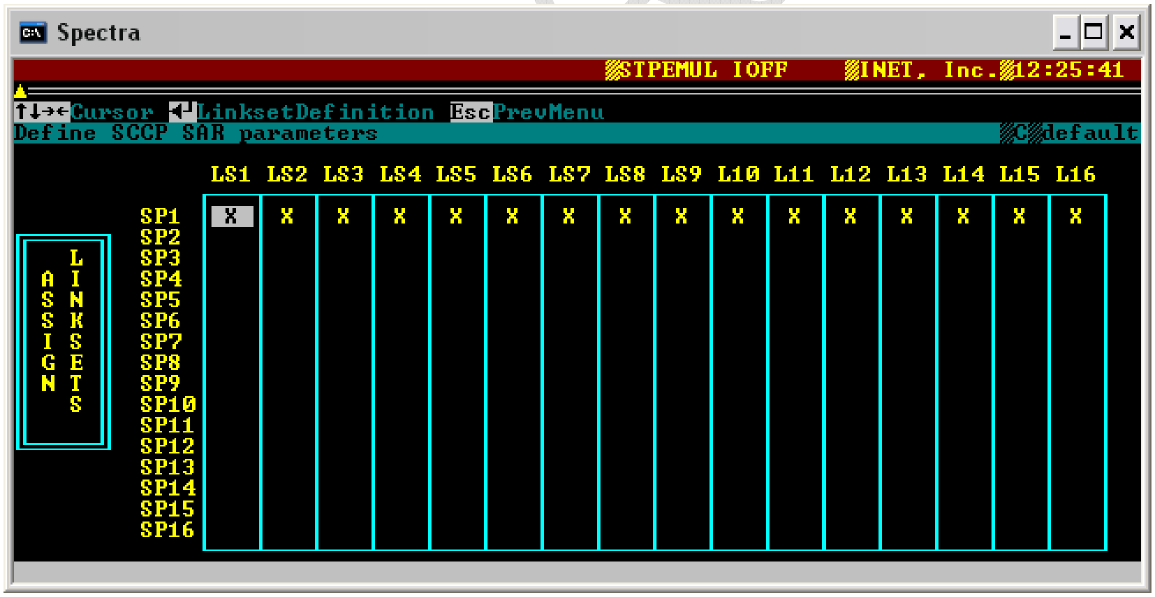
(b) Point codes and routes configured in this view.



```
Spectra
                                          ▒STPEMUL IOFF     ▒INET, Inc.▒12:25:08
Edit ↑↓→← CfgLinksets C-Link MoreParms VirtualSps Sp/Stp/SG/ASP TabForMore
Define SCCP SAR parameters                                          ▒C▒default
              Tester    Network

0-0-1        A SP   1  ├LS 1──────[SP ]  1-1-1
                       ├LS 2──────[SP ]  1-1-2
                       ├LS 3──────[SP ]  1-1-3
                       ├LS 4──────[SP ]  1-1-4
                       ├LS 5──────[SP ]  1-1-5
                       ├LS 6──────[SP ]  1-1-6
                       ├LS 7──────[SP ]  1-1-7
                       ├LS 8──────[SP ]  1-1-8
                       ├LS 9──────[SP ]  1-1-9
                       ├LS 10─────[SP ]  1-1-10
                       ├LS 11─────[SP ]  1-1-11
                       ├LS 12─────[SP ]  1-1-12
                       ├LS 13─────[SP ]  1-1-13
                       ├LS 14─────[SP ]  1-1-14
                       ├LS 15─────[SP ]  1-1-15
                       └LS 16─────[SP ]  1-1-16
```

Figure E-21. Configuration Level 3

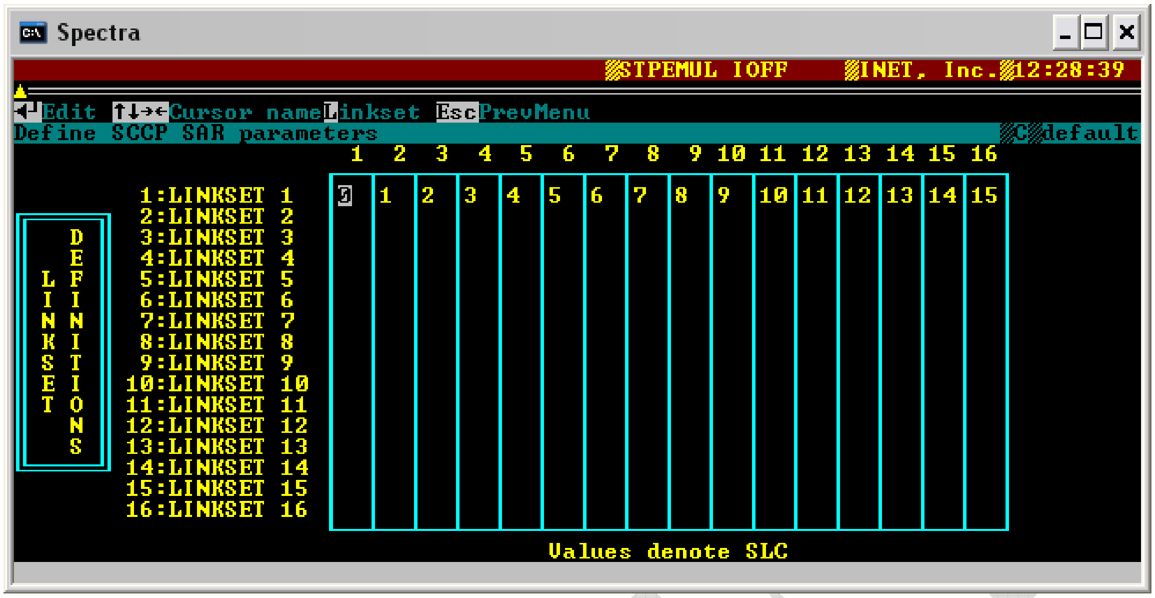
(c) Press “C” to configure LS on each Signaling Point (SP). See Figure E-22.



```
Spectra
                                          ▒STPEMUL IOFF     ▒INET, Inc.▒12:25:41
↑↓→←Cursor LinksetDefinition EscPrevMenu
Define SCCP SAR parameters                                          ▒C▒default

                LS1 LS2 LS3 LS4 LS5 LS6 LS7 LS8 LS9 L10 L11 L12 L13 L14 L15 L16

          SP1    X   X   X   X   X   X   X   X   X   X   X   X   X   X   X   X
          SP2
   L      SP3
 A I      SP4
 S N      SP5
 S K      SP6
 I S      SP7
 G E      SP8
 N T      SP9
   S      SP10
          SP11
          SP12
          SP13
          SP14
          SP15
          SP16
```

Figure E-22. Signaling Point

(d) From Figure E-22. Signaling Point view, press enter on any of the signaling points to define the signaling link code on a specific LS. See Figure E-23.

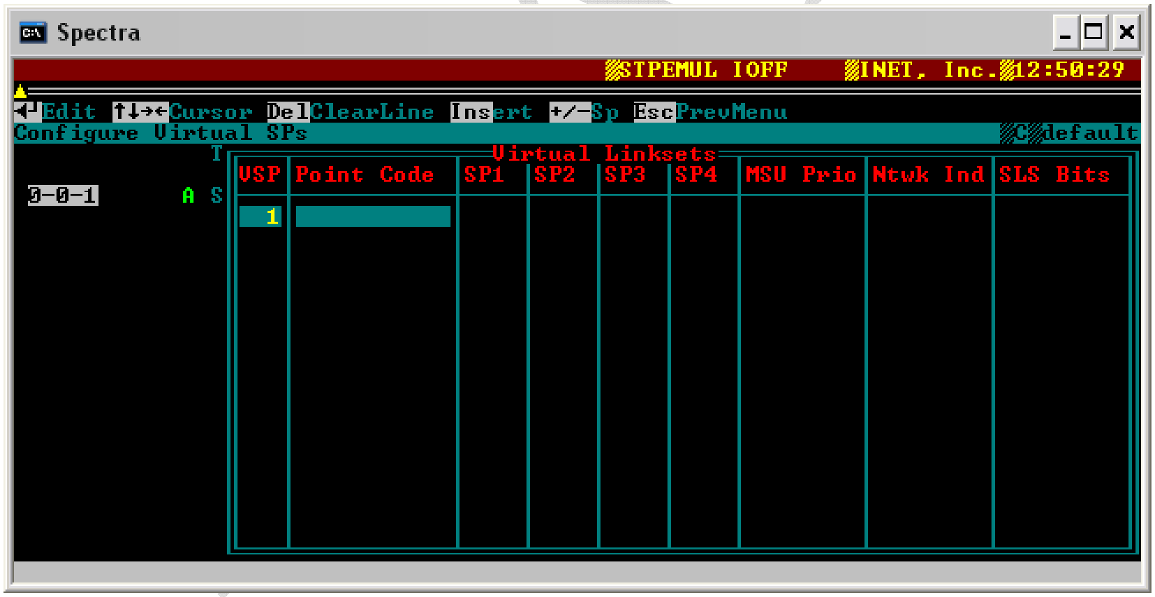


```
Spectra
                                       STPEMUL IOFF    INET, Inc. 12:28:39
Edit ↑↓→←Cursor name Linkset EscPrevMenu
Define SCCP SAR parameters                                       C default
                      1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16
         1:LINKSET 1  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
         2:LINKSET 2
    D    3:LINKSET 3
    E    4:LINKSET 4
  L F    5:LINKSET 5
  I I    6:LINKSET 6
  N N    7:LINKSET 7
  K I    8:LINKSET 8
  S T    9:LINKSET 9
  E I   10:LINKSET 10
  T O   11:LINKSET 11
    N   12:LINKSET 12
    S   13:LINKSET 13
        14:LINKSET 14
        15:LINKSET 15
        16:LINKSET 16
                              Values denote SLC
```

Figure E-23. Signaling Link Code

(e) Define virtual and/or remote point codes. See Figure E-24.

1. Instructions: From Figure E-6, press "V" to enter VSP.



```
Spectra
                                       STPEMUL IOFF    INET, Inc. 12:50:29
Edit ↑↓→←Cursor DelClearLine Insert +/-Sp EscPrevMenu
Configure Virtual SPs                                            C default
                T         Virtual Linksets
                  USP Point Code  SP1  SP2  SP3  SP4  MSU Prio Ntwk Ind SLS Bits
0-0-1         A S
                    1
```

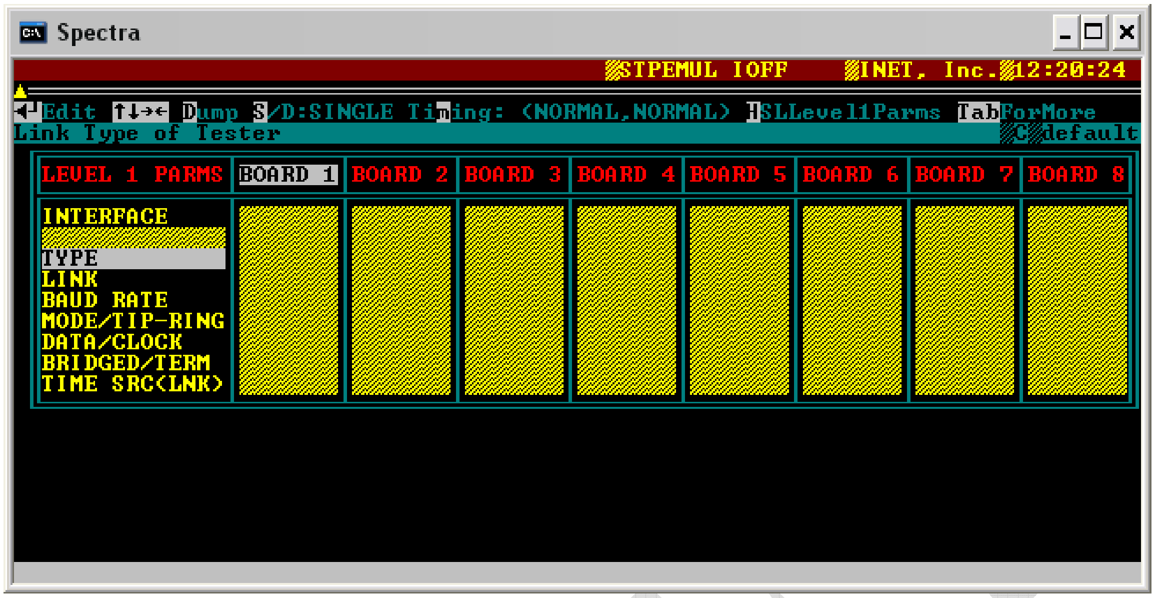
Figure E-24. Defining Point Codes

e. Configuring an ISDN Network

(1) Reference: Real Time Services Information Assurance Test Plan in Section E-7.2 RTS TDM Protocol Security Analysis Table E-15 Test Cases 1-4.

(2) Configure Level 1. See Figure E-25.

(a) Instructions: F1 → Level 1 Parameters → press enter.



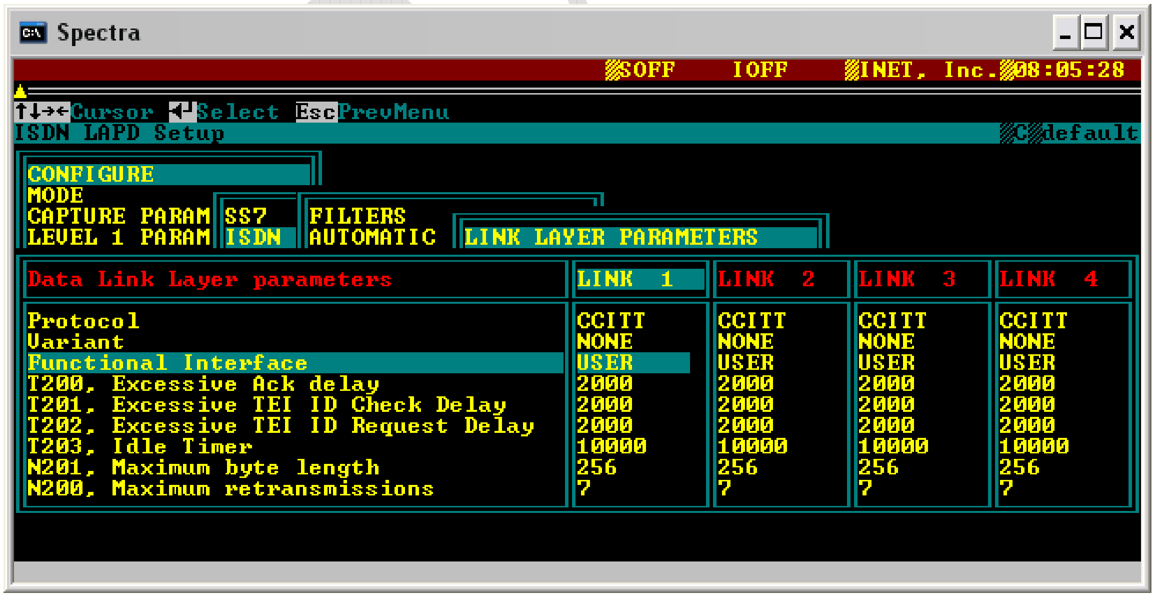
```
Spectra
                                              STPEMUL IOFF     INET, Inc. 12:20:24
↵Edit ↑↓→← Dump S/D:SINGLE Timing: (NORMAL,NORMAL) HSLLevel1Parms TabForMore
Link Type of Tester                                                      C default
 LEVEL 1 PARMS  BOARD 1  BOARD 2  BOARD 3  BOARD 4  BOARD 5  BOARD 6  BOARD 7  BOARD 8
 INTERFACE

 TYPE
 LINK
 BAUD RATE
 MODE/TIP-RING
 DATA/CLOCK
 BRIDGED/TERM
 TIME SRC(LNK)
```

Figure E-25. Configure Level 1

(3) Configure Level 2

(a) Instructions: F1 → Configure → ISDN → Level 2 Parameters → Link Layer Parameters. See Figure E-26.

(b) In this view, Configure “Protocol” to CCITT and “Functional Interface” to Network or User dependent on test scenario.



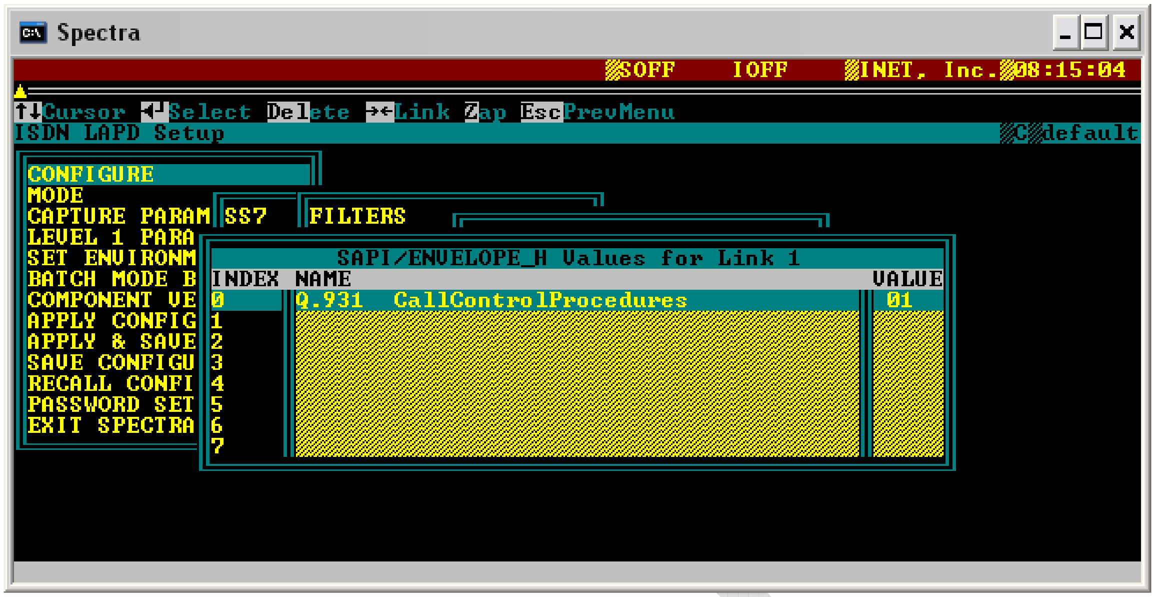
```
Spectra
                                              SOFF     IOFF     INET, Inc. 08:05:28
↑↓→←Cursor ↵Select EscPrevMenu
ISDN LAPD Setup                                                          C default
 CONFIGURE
 MODE
 CAPTURE PARAM  SS7   FILTERS
 LEVEL 1 PARAM  ISDN  AUTOMATIC   LINK LAYER PARAMETERS
```

Data Link Layer parameters	LINK 1	LINK 2	LINK 3	LINK 4
Protocol	CCITT	CCITT	CCITT	CCITT
Variant	NONE	NONE	NONE	NONE
Functional Interface	USER	USER	USER	USER
T200, Excessive Ack delay	2000	2000	2000	2000
T201, Excessive TEI ID Check Delay	2000	2000	2000	2000
T202, Excessive TEI ID Request Delay	2000	2000	2000	2000
T203, Idle Timer	10000	10000	10000	10000
N201, Maximum byte length	256	256	256	256
N200, Maximum retransmissions	7	7	7	7

Figure E-26. Configure Level 2

(c) Instructions: F1 → Configure → ISDN → Level 2 Parameters → SAPI assignments. See Figure E-26.1.

(d) In this view, define SAPI assignments for each link to Q.931. The SAPI is usually “0”.

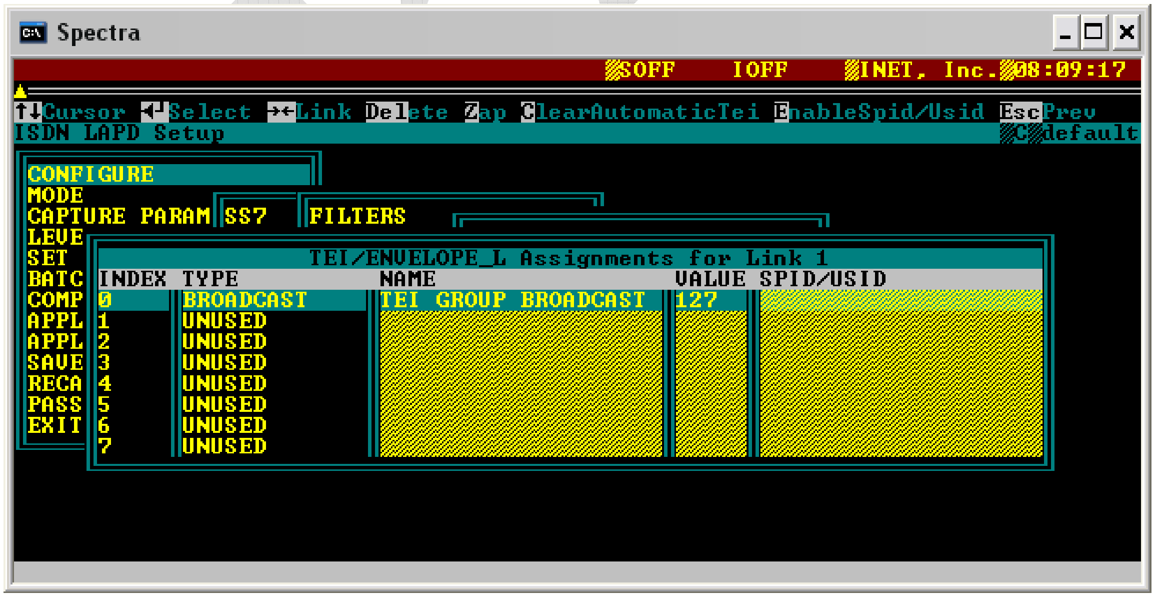


```
Spectra
                                   SOFF     IOFF     INET, Inc. 08:15:04
↑↓Cursor ↵Select Delete →←Link Zap EscPrevMenu
ISDN LAPD Setup                                                 C default
CONFIGURE
MODE
CAPTURE PARAM SS7    FILTERS
LEVEL 1 PARA
SET ENVIRONM        SAPI/ENVELOPE_H Values for Link 1
BATCH MODE B INDEX NAME                                         VALUE
COMPONENT VE 0     Q.931  CallControlProcedures                  01
APPLY CONFIG 1
APPLY & SAVE 2
SAVE CONFIGU 3
RECALL CONFI 4
PASSWORD SET 5
EXIT SPECTRA 6
             7
```

Figure E-26.1. Configure Level 2

(e) Instructions: F1 → Configure → ISDN → Level 2 Parameters → TEI assignments. See Figure E-26.2.

(f) In this view, press enter on an index other than the broadcast to define the TEI type, which is usually non-automatic. The TEI value is usually “0” or “1”.



```
Spectra
                                   SOFF     IOFF     INET, Inc. 08:09:17
↑↓Cursor ↵Select →←Link Delete Zap ClearAutomaticTei EnableSpid/Usid EscPrev
ISDN LAPD Setup                                                 C default
CONFIGURE
MODE
CAPTURE PARAM SS7    FILTERS
LEVE
SET            TEI/ENVELOPE_L Assignments for Link 1
BATC INDEX TYPE        NAME                  VALUE SPID/USID
COMP 0     BROADCAST   TEI GROUP BROADCAST   127
APPL 1     UNUSED
APPL 2     UNUSED
SAVE 3     UNUSED
RECA 4     UNUSED
PASS 5     UNUSED
EXIT 6     UNUSED
     7     UNUSED
```

Figure E-26.2. Configure Level 2

f. SS7 Examples

(1) SS7 Network Example Configuration. See Figure E-27.

(a) LS 1 with 4 links SLC 0,1,2,3 SP to SP.

(b) Refer to step d, Configuring a SS7 network, for assistance with configuration steps.

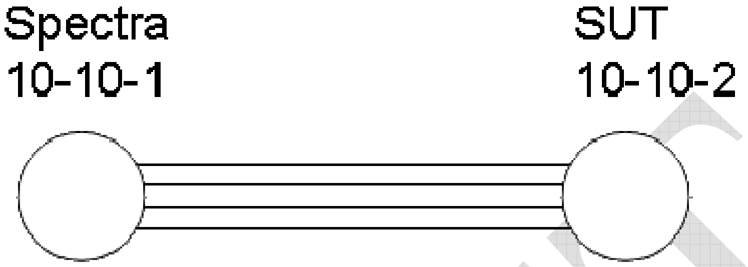


Figure E-27. SS7 Network Example Configuration

(2) SS7 Network Signaling Transfer Point (STP) Configuration. See Figure E-28.

(a) SP connecting to the STP SUT with remote point code.

(b) Instructions: LS 1, SLC 0,1.

(c) Refer to step d, Configuring a SS7 network, for assistance with configuration steps.

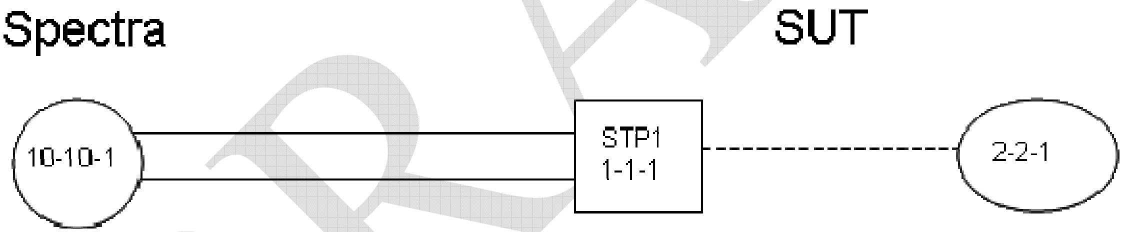


Figure E-28. SS7 Network STP Configuration 1

(3) SS7 Network STP Configuration. See Figure E-29.

(a) Pair of STPs connecting to the SUT.

(b) Instructions: LS 1, SLC 0,1.

(c) Refer to step d, Configuring a SS7 network, for assistance with configuration steps.

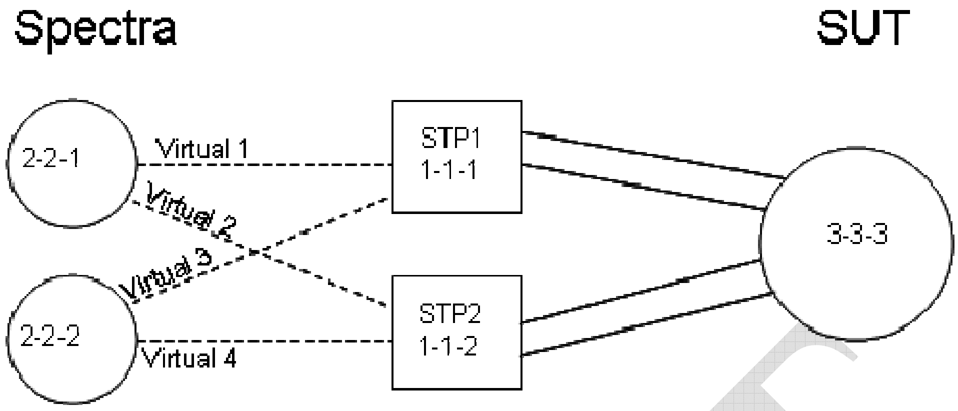


Figure E-29. SS7 Network STP Configuration 2

g. ISDN Examples

(1) ISDN Network Example Configuration. See Figure E-30.

(a) Spectra is TE (value 0).

(b) SUT is a Disk Management System or Media Gateway.

(c) Facility-Associated Signaling Primary Rate Interface (23B +D).

(d) Refer to step e, Configuring an ISDN network, for assistance with configuration steps.

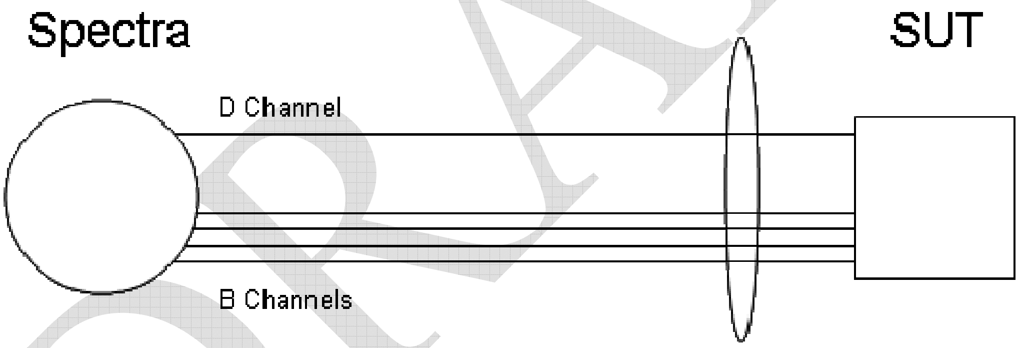


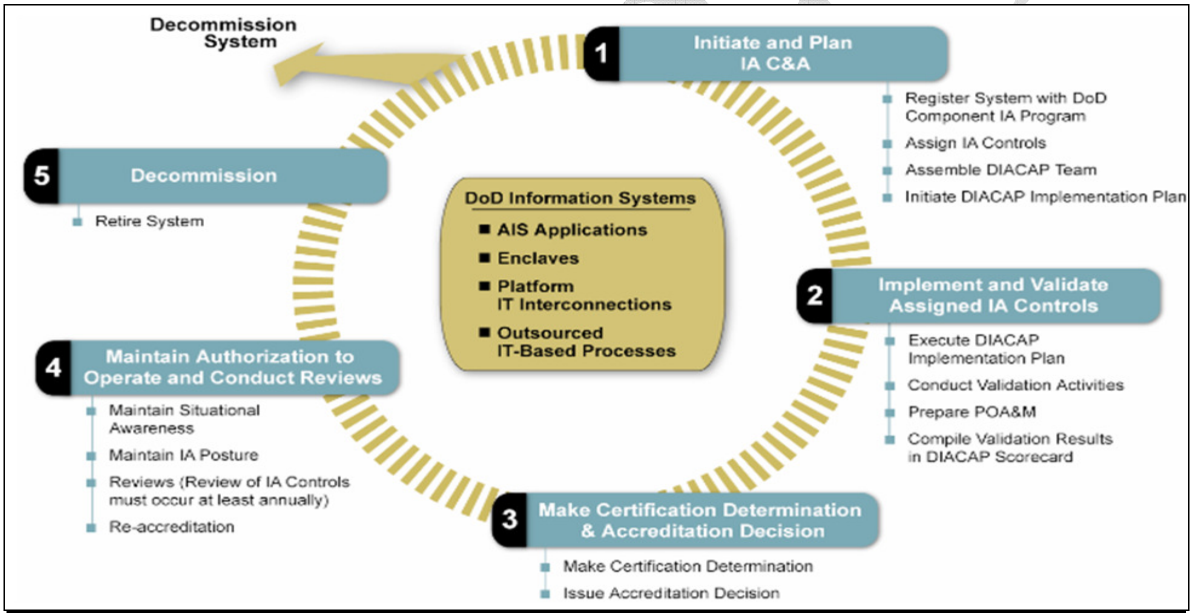
Figure E-30. ISDN Network Configuration

APPENDIX F

DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) PACKAGE

F-1. DEPARTMENT OF DEFENSE (DOD) INFORMATION ASSURANCE (IA) CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) PACKAGE

The DIACAP Package consists of a solution from the beginning of development until its decommission. The Joint Interoperability Test Command (JITC) IA Test Team (IATT) will be supporting the DIACAP Package through the first two stages of its lifecycle and preparing site installations for their DIACAP Package lifecycle of a Defense Switched Network Approved Products List solution. Figure F-1 shows the DIACAP Lifecycle.

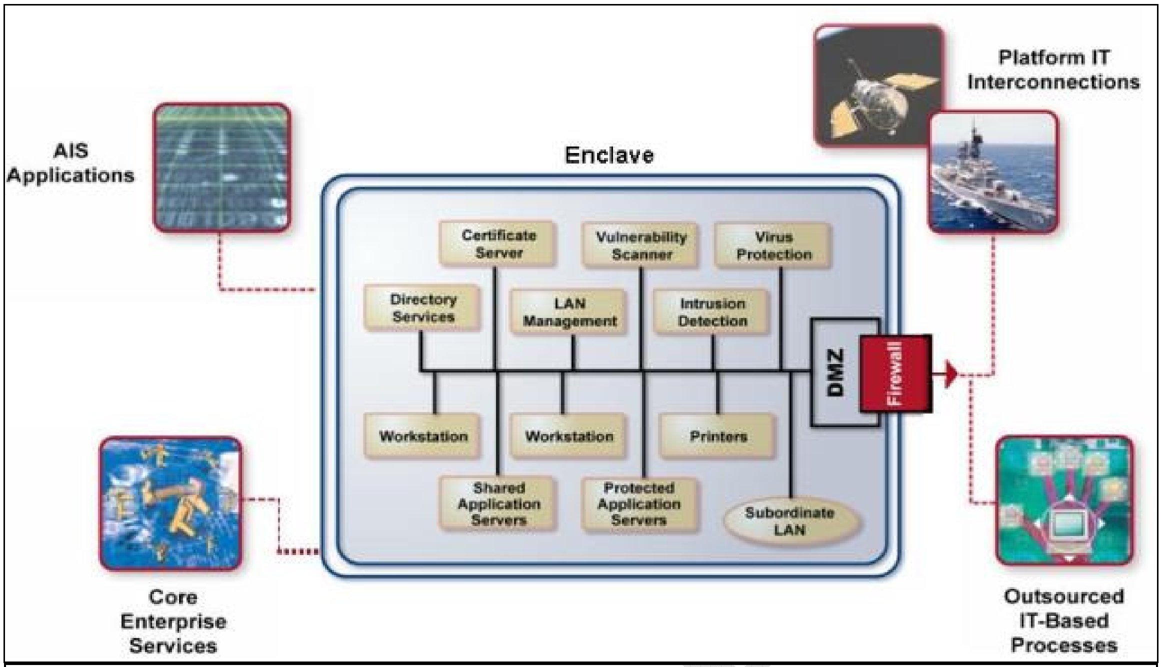

Decommission System
1
Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan
5
Decommission
Retire System
DoD Information Systems
AIS Applications
Enclaves
Platform IT Interconnections
Outsourced IT-Based Processes
2
Implement and Validate Assigned IA Controls
Execute DIACAP Implementation Plan
Conduct Validation Activities
Prepare POA&M
Compile Validation Results in DIACAP Scorecard
4
Maintain Authorization to Operate and Conduct Reviews
Maintain Situational Awareness
Maintain IA Posture
Reviews (Review of IA Controls must occur at least annually)
Re-accreditation
3
Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision

LEGEND:

AIS	Automated Information System	DoD	Department of Defense
C&A	Certification and Accreditation	IA	Information Assurance
DIACAP	DoD Information Assurance Certification and Accreditation Process	IT	Information Technology
		POA&M	Plan of Action and Milestones

Figure F-1. DIACAP Lifecycle

1. DoD Information Systems. All DoD Information Systems are divided into one of four portfolios, as shown in Figure F-2. The JITC IATT supports testing of many elements that can be components of a solution or complete solutions for supporting the warfighter.



LEGEND:

AIS	Automated Information System	IT	Information Technology
DMZ	Data Management Zone	LAN	Department of Defense

Figure F-2. DoD Information Systems

2. Accreditation Steps

a. Initiate and Plan IA Certification and Accreditation (C&A): The DIACAP registration is the activity by which DIACAP-related elements and system-unique attributes of the DoD information system are made visible to the governing Component IA Program for the purpose of tracking management indicators and for Federal Information Security Management Act (FISMA) reporting. Registration commences a dialog between the DoD information system and the governing DoD Component IA Program that continues until the DoD information system is decommissioned.

The set of information gathered during system registration is referred to as the System Identification Profile (SIP), which becomes part of the DIACAP Package for the information system and is maintained throughout the system's lifecycle. The SIP identifies the minimum data requirements, plus explanations, for registration. Typically, this information can be found in program/project documentation, such as the initial capabilities document, system requirements/specifications, architecture and design documents, etc.

The DIACAP Implementation Plan contains both the strategy for implementation along with the current implementation status of assigned IA Controls for a system. The plan is part of the DIACAP Package used by both the certifying authority and the designated accrediting authority for accreditation, and should be consistent with the program schedules.

The DIP should contain the following, minimum information:

- Assigned IA Controls - inherited and implemented
- Implementation Status
- Responsible entities
- Resources
- Estimated completion date for each IA Control

b. Implement and Validate Assigned IA Controls: A Plan of Action and Mitigation (POA&M) is prepared for DoD information systems with a current Authority to Operate that are found to be operating in an unacceptable IA posture through Government Accountability Office audits, Inspector General audits, or other reviews or events, such as an annual security review or compliance validation. The POA&M is a tool identifying tasks that need to be accomplished to remediate any identified vulnerabilities in a program or system. The POA&M addresses:

(1) Why the system needs to operate.
(2) Any operational restrictions imposed to lessen the risk during the interim authorization.
(3) Specific corrective actions necessary to demonstrate that all assigned IA Controls have been implemented correctly and are effective.
(4) The agreed upon timeline for completing and validating corrective actions.
(5) The resources necessary and available to properly complete the corrective actions.

c. Make Certification Determination & Accreditation Decision: A certification determination is made by a Certification Authority (CA). A CA representative is an active member of the DIACAP Team from inception and continuously assesses and guides the quality and completeness of DIACAP activities and tasks and the resulting artifacts. Certification considers:

(1) The IA posture of the DoD information system itself. That is, the overall reliability and viability of the information system plus the acceptability of the implementation and performance of IA mechanisms or safeguards that are inherent in the system itself; and,
(2) How the system behaves in the larger information environment, e.g., does it introduce vulnerabilities to the environment, does it correctly and securely interact with information environment management and control services, and is its visibility to situational awareness and network defense services adequate.

d. Maintain Authorization to Operate and Conduct Reviews: Not less than annually, the Information Assurance Manager (IAM) provides a written statement to the Designated Approving Authority (DAA) and the CA, based on the review of all IA Controls and testing of selected IA Controls as required by FISMA, which either confirms the effectiveness of assigned IA Controls and their implementation or recommends changes. The CA and DAA review the IAM statement, in light of mission and information environment indicators, and determine a course of action.

e. Decommission: When a DoD information system is removed from operation, a number of IA-related events are required relative to the disposition of DIACAP registration information and system–related data or objects in Global Information Grid (GIG) supporting IA infrastructures and core enterprise services such as key management, identity management, service management, privilege management, policy management, and discovery, as discussed in DoD Instruction (DoDI) 8500.2.

The program manager should coordinate with DoD governing GIG activities, as appropriate, to identify and apply applicable decommissioning requirements necessary to eliminate the functional or military capabilities of systems. Decommissioning requirements and procedures change over time as the GIG enterprise information environment changes and are maintained through the DIACAP Configuration Control Board and published in the DIACAP Knowledge Service.

APPENDIX G

REFERENCES

Department of Defense (DoD) Directive 8500.1 “Information Assurance (IA),” 24 October 2002

DoD Instruction (DoDI) 8500.2 “Information Assurance (IA) Implementation,” 6 February 2003

DoDI 8100.3, “Department of Defense Voice Networks,” 16 January 2004

DoDI 8551.1, “Port, Protocol and Services Management (PPSM),” 13 August 2004

Chairman of Joint Chiefs of Staff Instruction (CJCSI) 6211.02B, “DISN Connection Policy, Responsibilities, and Processes,” 31 July 2003

CJCSI 6212.01E, “Interoperability and Supportability of Information Technology and National Security Systems,” 15 December 2008

CJCSI 6215.01B, “Policy for Department of Defense Voice Services,” 23 September 2001

CJCSI 6510.01, “Information Assurance (IA) and Computer Network Defense (CND),” 12 August 2008

Assistant Secretary of Defense for Command, Control, Communications, Computers, and Intelligence/DoD Chief Information Officer Memorandum, Subject: “DoD Ports, Protocol, and Services Security Technical Guidance,” 5 November 2002

Executive Order 12333, “United States Intelligence Activities,” 4 December 1981

Committee on National Security Systems (CNSS) Instruction No. 4009, “National Information Assurance (IA) Glossary,” May 2003

Defense Information Systems Agency (DISA), “Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR), Incorporated Change 1,” 1 March 2005

DISA Security Technical Implementation Guides (STIG)

Joint Interoperability Test Command, “Defense Switched Network Generic Switch Test Plan (GSTP),” 23 April 2004

Telcordia GR-815-CORE, Issue 2, March 2002

American National Standard Institute (ANSI) T1.111 through T1.116, “Telecommunications Signaling System No. 7 (SS7),” 1992

National Institute of Standards and Technology (NIST) Special Publication, “Guideline on Network Security Testing”800-42 Special Publication SP 800-42, October 2003

NIST, “Creating a Patch and Vulnerability Management Program version 2” SP 800-40, November 2005

NIST, “Recommended Security Controls for Federal Information Systems” SP 800-53, December 2007

Federal Information Processing Standards Publications (FIPS Pubs) 140-2, 25 May 2001

Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Guidance, 28 November 2007

National Information Assurance Partnership (NIAP) version 1.02, March 2006

APPENDIX H

POINTS OF CONTACT

Napier, Michael
JITC Action Officer

JITC
ATTN: JTE/Napier
2001 Brainard Road/Bldg 57305
Fort Huachuca, AZ 85613
E-mail: Michael.Napier@disa.mil

(520) 538-6787
DSN 879-6787
Fax (520) 538-4347

Quick-Keckler, Donna
UC IA Test Manager

JITC
ATTN: NGIT/Quick-Keckler
2001 Brainard Road
Fort Huachuca, AZ 85613
E-mail: Donna.Quick-Keckler.ctr@disa.mil

(520) 538-4537
DSN 879-4537
Fax (520) 538-5258

Searle, Brent
UC IA IPV Team Lead

JITC
ATTN: NGIT/CSC/Searle
2001 Brainard Road
Fort Huachuca, AZ 85613
E-mail: Brent.Searle.ctr@disa.mil

(520) 538-2591
DSN 879-2591
Fax (520) 538-5258

Gardner, Lorraine
UC IA STIG Team Lead

JITC
ATTN: NGIT/Gardner
2001 Brainard Road
Fort Huachuca, AZ 85613
E-mail: Lorraine.Gardner.ctr@disa.mil

(520) 538-2578
DSN 879-2578
Fax (520) 538-5258

(The page intentionally left blank.)